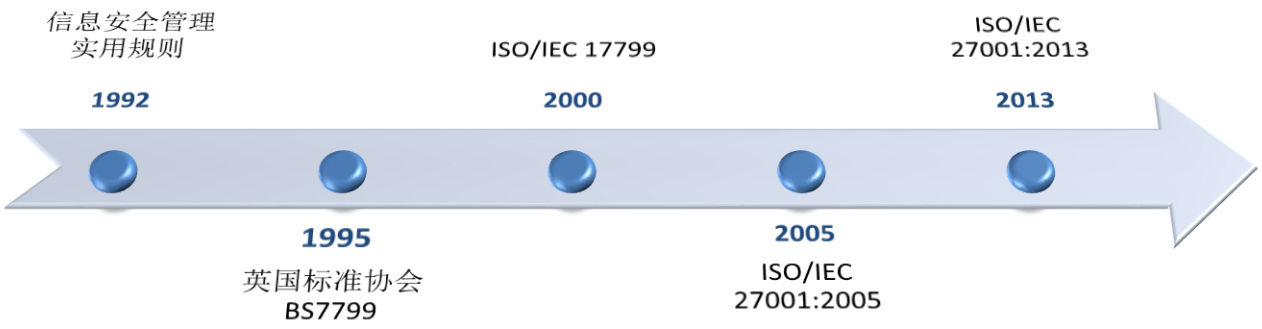
信息安全管理体系
ISO/IEC 27000 标准系列概论



什么是 ISO/IEC 27001？

ISO/IEC 27001 标准的名称为《信息技术 — 安全技术 — 信息安全管理体系 — 要求》，由国际标准化组织（ISO）及国际电工委员会（IEC）出版。ISO/IEC 27001:2013（下称 ISO/IEC 27001）为最新版本的 ISO/IEC 27001 标准，修订了 2005 年出版的上一个版本（即 ISO/IEC 27001:2005）。本标准订明有关建立、推行、维护和持续改进信息安全管理体系的各项要求。信息安全管理体系阐述保护敏感信息安全的系统化方式，通过应用风险管理流程管理人事、工序及信息技术系统。这套系统不仅适用于大型机构，中小型企业也会合用。

ISO/IEC 27001 可以与相关支援控制措施配合使用，例如载列于 ISO/IEC 27002:2013（下称 ISO/IEC 27002）文件的控制措施。ISO/IEC 27002 分为 14 节及 35 个控制目标，详述 114 项安全控制措施。有关 ISO/IEC 27001 及 ISO/IEC 27002 的目录载于附录 A。

机构是否遵行 ISO/IEC 27001 标准所定的要求，可由认可认证机构进行正式评估和认证。若机构的信息安全管理体系获取 ISO/IEC 27001 标准的认证，显示机构致力保护信息安全，又可增加客户、合伙人及持份者的信心。

ISO/IEC 27001 认证要求

为符合 ISO/IEC 27001 认证要求，机构的信息安全管理体系必须由国际认可的认证机构进行审计。ISO/IEC 27001 第 4 节至 10 节所载的要求（见附录 A）是强制性要求，并没有豁免情况。若机构的信息安全管理体系通过正式审计，便会获认证机构颁发 ISO/IEC 27001 证书。证书的有效期为三年，期满后，机构需要重新为其信息安全管理体系进行认证。

在三年有效期内，机构必须执行证书维护，以确保信息安全管理体系持续遵行有关要求，按规定运行和不断改进。为了保持证书有效，认证机构会每年至少一次就信息安全管理体系进行实地视察，以进行监察审计。在审计过程中，认证机构只会对部分信息安全管理体系作出审计。当三年有效期临近届满时，认证机构才会对整个信息安全管理体系作出审计。

ISO/IEC 27001 认证的效益

机构获取 ISO/IEC 27001 认证后，在内部安全及对外竞争力方面，均会受惠。

在内部方面，机构采用 ISO/IEC 27001 可获得下述效益：

- 订立依据，以便安全地交换信息和保护数据隐私，尤其是敏感信息；
- 管理和减低风险承担，从而减少发生事件的机会，亦相应减少用于安全事件应变的时间及金钱；
- 加强内部组织架构和改进业务的安全性结构，如明确界定有关信息安全的职责及职务；
- 减少在投标合约时和批出合约后，按客户的要求分别用于整理和提交与安全相关信息的资源。

在对外方面，机构通过宣传已获取 ISO/IEC 27001 认证，可获得下述效益：

- 给予客户及持份者信心，让他们了解机构如何管理敏感信息的风险及安全事宜；
- 有助遵守法律责任，如《个人资料（私隐）条例》；
- 享有竞争优势，以助吸引更多投资者及客户；
- 改进服务及产品的一致性，从而提高客户的满意度和挽留客户；
- 由于安全流程经独立认证机构核实，故可保护和提升机构信誉，从而提高对机构、资产、股东及董事的保护；
- 充分准备好面对客户日益殷切的期望。现时市民对信息安全事件愈趋敏感，一个认可国际标准认证或会渐渐成为客户采用服务的先决条件。

认证机构

ISO/IEC 27001 认证过程涉及由认证机构给予的认可。认证机构须显示已完全符合有关国际标准的要求，即 ISO/IEC 17021《合格评定 — 管理体系审核认证机构的要求》及 ISO/IEC 27006《信息安全管理体系审核认证机构的要求》，才获授予认可。

2011 年 11 月 15 日，香港认可处正式推出 ISO/IEC 27001 认证的认可服务。认证机构可联络香港认可处，并提出认可申请。有关申请纯属自愿性质。

认证费用

首次认证费用包括推行信息安全管理体系和获取 ISO/IEC 27001 认证所需的费用。推行信息安全管理体系的费用，主要取决于机构现有与所需的安全控制措施之间的差距。在推行费用方面，部分费用及资源用于推行安全控制措施、编写文档、培训人员等。获取认证的费用则包括外聘审计人员费用（每天按一定比例收取的费用）、申请费、证书费、维护费等。

香港的应用情况

根据国际标准化组织在 2016 年进行的调查，全球 140 个国家及经济体系已获发至少 33 290 张 ISO/IEC 27001 证书。在 2016 年，首三个获发证书总数最多的国家分别是日本（8 945 张）、英国（3 367 张）及印度（2 902 张）。根据同一调查的数据，香港获发的证书数目为 173 张，包括部分政府部门就某些指定职能范畴取得的 ISO/IEC 27001 认证。

ISO/IEC 27001 的推行情况和认证过程概要

- **ISO/IEC 27001的推行情况**

1. **制订信息安全方针**
   - 工作：确定业务目标并取得管理层的支持，以推行安全改进计划。
2. **界定信息安全管理体系范围**
   - 工作：比较现有的信息安全管理体系与ISO/IEC 27001的要求，同时选择信息安全管理体系将会涵盖的业务单位、部门或系统。
3. **进行风险评估**
   - 工作：制订风险评估的方法，备存须予保护的信息资产清单，并按风险评估的风险分类排列资产。
4. **管理已确定的风险**
   - 工作：建立风险处理计划，为信息安全风险管理确立适当的管理工作、资源、职责及优先事项。
5. **选择将会推行的控制措施**
   - 工作：拟备适用性声明，记录适用于信息安全管理体系的控制措施（例如ISO/IEC 27002中的114项安全控制措施）及这些措施的推行方法。
6. **推行控制措施**
   - 工作：制定计划以推行已确定的控制措施。

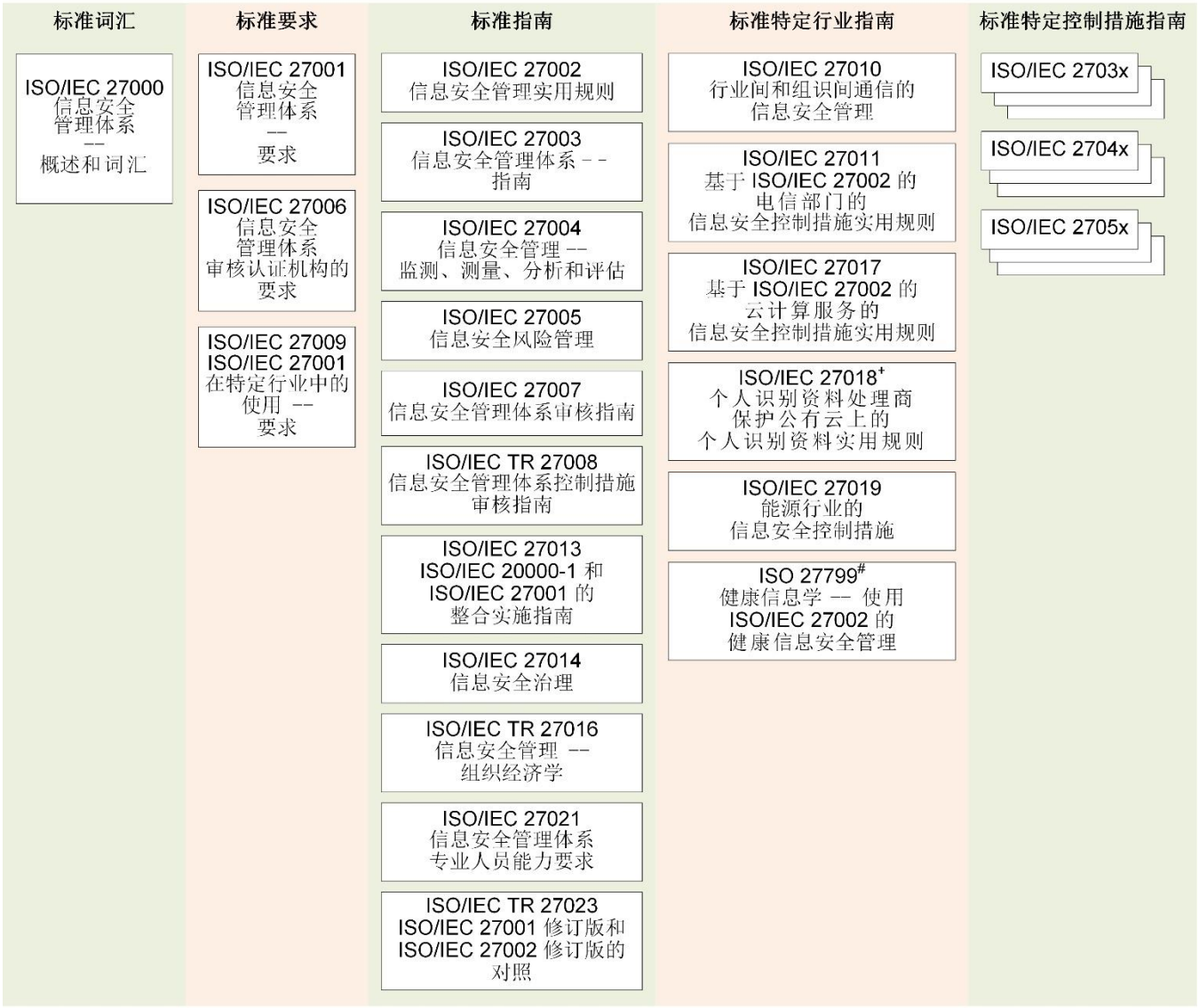
- **ISO/IEC 27001的认证**

7. **准备认证**
   - 工作：操作信息安全管理体系，并进行包括内部审计、管理覆检和其它相关工作的整个流程。
8. **申请认证**
   - 工作：着手申请认证，其中包括在不同阶段的档案覆检及有关遵行要求的实地审计。

ISO/IEC 27000 标准系列

ISO/IEC 27000 标准系列（见附录 B）包括互有关连的标准及指南(已经出版或正在拟备)，以及若干重要的组成部分。这些组成部分重点介绍有关信息安全管理体系要求（ISO/IEC 27001）、ISO/IEC 27001 标准的认证机构要求（ISO/IEC 27006）及信息安全管理系统于特定行业推行的外加要求框架（ISO/IEC 27009）的参考标准。其它标准及指南就推行信息安全管理体系的不同范畴提供指引，如一般流程、特定控制措施指南及特定行业指南。

ISO/IEC 27000 标准系列的关系



备注：
并非使用同一通用名称的国际标准，但属ISO/IEC 27000系列的标准
+ 内地名称：公有云服务的数据保护控制实用规则

ISO/IEC 27001 的现有版本在 2013 年发布。除了上文最多提及的 ISO/IEC 27001、ISO/IEC 27002 及 ISO/IEC 27018 外，ISO/IEC 27000 标准系列的一些其它标准也被广泛引用。例子包括：

- ISO/IEC 27000 —《信息安全管理体系 — 概述和词汇》概述信息安全管理体系的数据，并提供信息安全管理体系标准系列的常用术语和定义。为确保用语一致，所有ISO/IEC 27000标准系列会以ISO/IEC 27000所载的术语及定义为准。这标准提供入门概览，让读者对ISO/IEC 27000标准系列有初步了解。

- ISO/IEC 27003 —《信息安全管理体系 — 指南》就ISO/IEC 27001所订明对信息安全管理体系的要求提供指南，并载述与这些要求相关的建议、可能情况及允许情况。

- ISO/IEC 27004 —《信息安全管理 — 监测、测量、分析和评估》提供指引，协助机构评估信息安全绩效和信息安全管理体系的成效，以达到ISO/IEC 27001:2013所订明有关监测、测量、分析和评估的要求。

- ISO/IEC 27005 — 《信息安全风险管理》提供有关信息安全风险管理的指南。该标准进一步阐述ISO/IEC 27001所载的一般概念，旨在协助按风险管理方法顺利推行信息安全措施。

- ISO/IEC 27017 —《基于ISO/IEC 27002的云计算服务的信息安全控制措施实用规则》提供支援推行信息安全控制措施并适用于云用户及供应商的指南。用户及供应商可按照适用于云服务的风险评估及其它要求，选择适当的控制措施和采用有关的推行指南。这标准与ISO/IEC 27018一并使用，涵盖范围更为广泛，除隐私外，还包括云计算的信息安全方向。

- ISO/IEC 27031 —《信息及通信技术业务连续性就绪指南》说明有关促进业务连续性的信息及通信技术就绪程度概念及原则，并提供相关方法及流程的框架，以识别和订明可提升机构信息及通信技术就绪程度的措施，以促进业务连续性。

- ISO/IEC 27035-1 —《信息安全事件管理 — 第1部分：事件管理原则》载述信息安全事件管理的基本概念及各个阶段，并有系统地将这些概念与原则结合，用于事件检侦、报告、评估和响应，以及经验教训。

- ISO/IEC 27035-2 —《信息安全事件管理 — 第2部分：规划和准备事件响应指南》就事件响应的规划和准备提供指南。

- ISO/IEC 27036-4 —《供应商关系信息安全 — 第4部分：云服务安全指南》制订支援推行信息安全管理体系并适用于云服务的指南。

- ISO/IEC 27037 —《数字证据的标识、收集、获取和保存指南》提供指南，说明处理数字证据的具体工作，包括标识、收集、获取和保存或具证据价值的潜在数字证据。

云计算中的个人识别资料

目前，云计算以前所未有的方式不断演变，这个趋势在未来数年将会持续和继续发展。云计算具备潜在的好处，在使用、维护和提升方面亦具备成本效益。较诸传统的数据存储方法，云计算的数据备份和复原方法亦较为容易。此外，云计算亦具备快速配置和便利获取信息的好处。

一些机构将应用系统迁移到云。从机构的角度来看，云计算的安全，尤其是数据安全和隐私保护等问题备受关注，这些仍然是阻碍机构采用云计算服务的主要因素。

ISO/IEC 27018:2014 标准（下称 ISO/IEC 27018）的名称为《个人识别资料处理商保护公有云上的个人识别资料实用规则》(内地名称：《公有云服务的数据保护控制实用规则》)。这是首个专为保护公有云上个人数据而设的国际标准。ISO/IEC 27018 主要阐述普遍用作保护经公有云服务供应商(即个人识别资料处理商)处理的个人识别资料的控制目标、控制措施和指南。

ISO/IEC 27018 为通过云处理个人识别资料的所有类型及规模的私营或公营机构(个人识别资料处理商) 而设。

ISO/IEC 27018 的保护个人识别资料控制措施

制订 ISO/IEC 27018 时已考虑 ISO/IEC 27002 所载的要求，并通过以下两种方法加强 ISO/IEC 27002 的内容：第一，就 ISO/IEC 27002 所订明的控制措施实施指南作出补充；第二，提供 ISO/IEC 27002 未有涵盖的额外控制措施和相关的实施指南，以配合保护在公有云上的个人识别资料的要求。就第一种方法而言，ISO/IEC 27018 在以下 11 项 ISO/IEC 27002 控制措施制订了额外的实施指南：

- 信息安全方针
- 信息安全组织架构
- 人力资源安全
- 访问控制
- 加密方法
- 物理与环境安全
- 操作安全
- 通信安全
- 信息安全事件管理
- 信息安全方面的业务连续性管理
- 符合性

就第二种方法而言，ISO/IEC 27018 附件 A 载列 11 项在 ISO/IEC 27002 基础上的加强控制措施，以符合保护个人识别资料的要求，该等要求适用于作为个人识别资料处理商的公有云服务供应商。这些加强控制措施根据 ISO/IEC 29100《信息技术 — 安全技术 — 隐私框架》的 11 项隐私原则分类。有关 ISO/IEC 29100 的隐私原则载于附录 A。

ISO/IEC 27018 的效益

ISO/IEC 27018 适用于处理从用户获取的个人识别资料，以作用户与云服务供应商所订立的合约中已订明的用途。通过采用 ISO/IEC 27018，机构可：

- *用作指引，以便遵行有关保护数据的要求；*
- *赢取客户的信任，以便他们把数据托管于云平台，从而拓展客源；以及*
- *协助在跨国市场营运的公有云服务供应商符合不同国家的保护数据标准，并在不同司法管辖区进行复杂评估。*

后记

ISO/IEC 27001 阐述信息安全管理体系的正式规格，着重于「管理体系」而非「信息安全」。已认证的信息安全管理体系能明确显示该机构正通过系统化方法鉴别、评估和管理信息安全风险。信息安全管理体系若能有效操作，则可确保已采取足够的安全控制措施。ISO/IEC 27001 证书可有助推广、提高公信力和增加客户信心。

附录 A

ISO/IEC 27001:2013 的目录

0. 简介
1. 范围
2. 参考标准
3. 术语和定义
4. 组织架构环境
5. 领导力
6. 策划
7. 支援
8. 运行
9. 绩效评价
10. 改进

附件 A 控制目标和控制措施参考〈标准〉
参考文献

ISO/IEC 29100 的隐私原则

1. 同意与自主
2. 利用目的之合法性与阐明该目的
3. 搜集限制
4. 资料最小化
5. 利用、保存与揭露之限制
6. 正确性与品质
7. 公开、透明与告知
8. 当事人参与和访问
9. 相关责任
10. 信息安全
11. 遵守隐私

ISO/IEC 27002:2013 的目录

0. 简介
1. 范围
2. 参考标准
3. 术语和定义
4. 本标准的结构
5. 信息安全方针
6. 信息安全组织架构
7. 人力资源安全
8. 资产管理
9. 访问控制
10. 加密方法
11. 物理与环境安全
12. 操作安全
13. 通信安全
14. 系统购置、发展和维护
15. 供应商关系
16. 信息安全事件管理
17. 信息安全方面的业务连续性管理
18. 符合性

参考文献

附录 B

以下 ISO/IEC 27000 标准系列的信息安全标准已经出版或正在拟备：
（注：TR 指技术报告）

标准	出版	名称
ISO/IEC 27000	2016*	信息安全管理体系 — 概述和词汇
ISO/IEC 27001	2013	信息安全管理体系 — 要求
ISO/IEC 27002	2013	信息安全管理实用规则
ISO/IEC 27003	2017	信息安全管理体系 — 指南
ISO/IEC 27004	2016	信息安全管理 — 监测、测量、分析和评估
ISO/IEC 27005	2011*	信息安全风险管理
ISO/IEC 27006	2015	信息安全管理体系审核认证机构的要求
ISO/IEC 27007	2017	信息安全管理体系审核指南
ISO/IEC TR 27008	2011*	信息安全管理体系控制措施审核指南
ISO/IEC 27009	2016*	ISO/IEC 27001 在特定行业中的使用 — 要求
ISO/IEC 27010	2015	行业间和组织间通信的信息安全管理
ISO/IEC 27011	2016	基于 ISO/IEC 27002 的电信部门的信息安全控制措施实用规则
ISO/IEC 27013	2015	ISO/IEC 20000-1 和 ISO/IEC 27001 的整合实施指南
ISO/IEC 27014	2013*	信息安全治理
ISO/IEC TR 27016	2014	信息安全管理 — 组织经济学
ISO/IEC 27017	2015	基于 ISO/IEC 27002 的云计算服务的信息安全控制措施实用规则
ISO/IEC 27018	2014	个人识别资料处理商保护公有云上的个人识别资料实用规则(内地名称：公有云服务的数据保护控制实用规则)
ISO/IEC 27019	2017	能源行业的信息安全控制措施
ISO/IEC 27021	2017	信息安全管理体系专业人员能力要求
ISO/IEC TR 27023	2015	ISO/IEC 27001 修订版和 ISO/IEC 27002 修订版的对照
ISO/IEC 27031	2011	信息及通信技术业务连续性就绪指南
ISO/IEC 27032	2012	网际安全指南
ISO/IEC 27033-1	2015	网络安全 — 第 1 部分：概述和概念
ISO/IEC 27033-2	2012	网络安全 — 第 2 部分：网络安全设计和实施指南
ISO/IEC 27033-3	2010	网络安全 — 第 3 部分：参考网络场景 — 威胁、设计技术和控制问题
ISO/IEC 27033-4	2014	网络安全 — 第 4 部分：使用安全网关的网络之间的安全通讯
ISO/IEC 27033-5	2013	网络安全 — 第 5 部分：使用 VPN 的网络间的安全通信
ISO/IEC 27033-6	2016	网络安全 — 第 6 部分：无线 IP 网络访问安全
ISO/IEC 27034-1	2011	应用安全 — 第 1 部分：概述和概念
ISO/IEC 27034-2	2015	应用安全 — 第 2 部分：组织规范性框架

标准	出版	名称
ISO/IEC 27034-3	拟稿^	应用安全 — 第 3 部分：应用安全管理过程
ISO/IEC 27034-5	2017	应用安全 — 第 5 部分：协议和应用安全控制措施数据结构
ISO/IEC 27034-6	2016	应用安全 — 第 6 部分：个案研究
ISO/IEC 27035-1	2016	信息安全事件管理 — 第 1 部分：事件管理原则
ISO/IEC 27035-2	2016	信息安全事件管理 — 第 2 部分：规划和准备事件响应指南
ISO/IEC 27035-3	拟稿^	信息安全事件管理 — 第 3 部分：事件响应操作指南
ISO/IEC 27036-1	2014	供应商关系信息安全 — 第 1 部分：概述和概念
ISO/IEC 27036-2	2014	供应商关系信息安全 — 第 2 部分：要求
ISO/IEC 27036-3	2013	供应商关系信息安全 — 第 3 部分：ICT 供应链安全指南
ISO/IEC 27036-4	2016	供应商关系信息安全 — 第 4 部分：云服务安全指南
ISO/IEC 27037	2012	数字证据的标识、收集、获取和保存指南
ISO/IEC 27038	2014	数字编辑规范
ISO/IEC 27039	2015	入侵检测防御系统的选择、部署和操作
ISO/IEC 27040	2015	存储安全
ISO/IEC 27041	2015	确保事件调查方法适合性和充分性的指南
ISO/IEC 27042	2015	数字证据的分析和解释指南
ISO/IEC 27043	2015	事件调查原则和过程
ISO/IEC 27050-1	2016	电子发现 — 第 1 部分：概述和概念
ISO/IEC 27050-2	拟稿^	电子发现 — 第 2 部分：电子发现管治和管理指南
ISO/IEC 27050-3	2017	电子发现 — 第 3 部分：电子发现实务守则
ISO 27799 #	2016	健康信息学 — 使用 ISO/IEC 27002 的健康信息安全管理

^ 拟备中

* 正进行调整

并非使用同一通用名称的国际标准，但属 ISO/IEC 27000 系列的标准

参考资料

1. 参考 http://www.iso.org
   有关 ISO/IEC 27000 标准系列的内容
2. 参考 http://www.pc-history.org/17799.htm
   有关 ISO/IEC 27001 的演变
3. 参考 http://www.iso.org/iso/home/standards/certification
   有关 ISO 证书调查报告

「云资讯网」是一站式入门网站，由云端运算服务和标准专家小组建立，方便市民和企业（特别是中小企）有效取得有关云计算技术的信息和资源。该网站提供用例、相关指引和良好作业模式，让市民和企业在采用云计算模式时达到预期效益。

云端运算服务和标准专家小组由香港特区政府属下的政府资讯科技总监办公室成立，通过广纳业界、学术界、专业团体及政府的专业知识，推动香港云计算的应用和发展，以及促进本港云计算专家彼此交流及与内地专家互相交流。云端保安及私隐工作小组是一个在专家小组辖下设立的工作小组。

工作小组成员通过通力合作，制订有关措施，以推动并促进本地业界，更广泛应用云计算和安全使用云服务。