第二部分 建立合规

第四章　隐私合规框架

虽然理解 GDPR 的基础知识是一个好的开始，但合规项目一开始的几个步骤仍然是最让人困惑的。你要从哪里开始？谁需要参与？如何确定并履行你的所有义务？如何证明你符合该条例的所有要求？

这类问题会分散你对项目核心需求的注意力，并让整个过程看起来无比艰巨。

对于大多数组织来说，一个更简单的做法或许是暂时不去管 GDPR 中那些具体的、详细的要求，而是从建立一个框架开始，以确保当下和未来数年的合规。GDPR 特别要求控制者应“基于对处理的性质、范围、背景和目的，以及自然人的权利和自由所受的不同可能性和严重性的风险等方面的考虑……采取适当的技术和组织措施，以确保并能够证明处理遵循条例进行。必要时还应审查和更新这些措施”。[68] 该条款实际上是说，组织应该建立一个合规框架来确保其采用了适当的技术和组织措施，以确保数据处理按 GDPR 合规的方式进行。

GDPR 还明确要求组织证明他们已将“基于设计与默认的数据保护”原则嵌入了他们的组织文化中。虽然要有一些必要的具体步骤来嵌入预设的数据保护，但其起点无疑是建立一个适当的合规框架，以确保数据

[68]　GDPR，第 24（1）条。

保护处于组织行为的核心。

一个“合规框架”是一套结构化的指南和实践，把适用于一个组织的一般合规要求和满足这些要求所必需的业务流程、政策和控制结合在一起。相关的技术措施包括具体的程序，以及员工培训、审计和所有相关的技术性和物理性安全控制，这些构成了一个有效的信息安全管理体系的一部分。有关的这些流程、策略和控制在大体上勾勒出组织如何管理与合规要求有关的沟通、风险和治理手段。由于不同的合规要求之间往往会有一些重叠，因此框架应对此做出识别，以消除由此带来的冗余和不确定性。

所有合规框架都将包括三类活动：人员、流程和技术，如图 1 所示。

针对任何立法、监管或合同要求都可以制定一个合规框架。对于 GDPR 来说，这一框架显然是指向一个隐私合规框架。

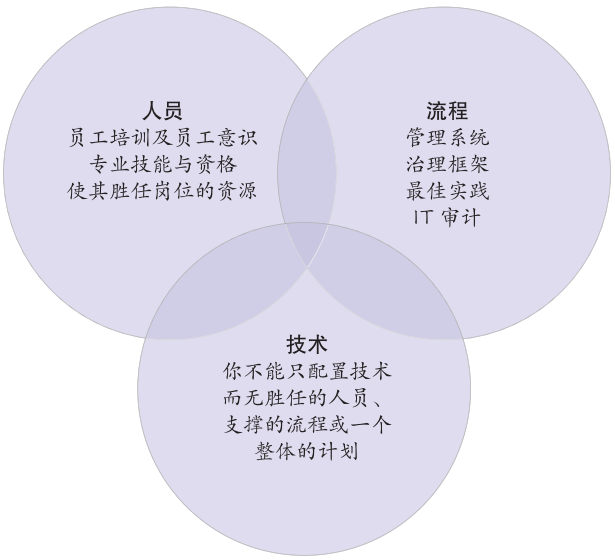

图 1　三类活动：人员、流程和技术

隐私合规框架的开发可参比任何其他进行中的项目。你会希望建立一套策略与实践，确保特定的处理能始终遵循它。假设这些处理符合法律要求，那么该框架就应确保组织始终守法。重要的是，不必从一开始就定义所有的处理：它们可以适时地在不同阶段纳入框架以实现合规。最重要的一步是建立一个初始的框架。

完成该任务有两种方法：完全由自己构建，或者运用和调整一个公开的合规框架。第一种选择依赖于一些试错和（可能昂贵的）咨询支持；第二种选择利用既有的最佳实践，可能比自己来做能更快、更具成本效益地达到合规。

有几个合规框架和标准可供选择。GDPR 明确指出，使用国际标准和隐私标记（Privacy marks）是证明合规的有效工具，借由这类既有的最佳实践来启动一个隐私合规项目具备实操性和商业意义。

隐私合规框架之所以有用，主要是因为它提供了一种管理机密数据的结构化方式，使组织能够遵守那些复杂的法律，甚至能针对不同的司法管辖区来遵守。尚未建立隐私合规框架的组织可以使用标准化框架，实现从风险敞露到合规的飞跃；已经建立了隐私合规框架的组织可以使用国内和国际的标准来获取认证，这些认证将提高你与客户及利益相关方之间的信任，并向监管机构或法院证明，你已经做到了尽职与合规的努力。目前有两个被认可的标准或框架可使用：ISO/IEC 27001:2013 结合 ISO/IEC 27701:2019，以及 BS 10012:2017。目前 ISO 27001 已有国际认可的认证计划，而 BS 10012 认证则主要由英国提供。其他标准和信任标记（Trust marks）也预计会出现。

隐私合规框架的三个关键领域是：

1. 治理手段、风险管理与合规目标；
2. 数据处理原则；
3. 政策、程序、控制和记录。

在大多数管理体系和框架中普遍都有一种认知，即流程之间是相互联系的，它们都通过一组共同的控制过程来进行输入和获得反馈。也就是说，与大多数的业务流程一样，框架和系统将定义好输入和输出，有符合隐私规定的输入，就会有符合隐私规定的输出。

属事范围

任何框架都有一个特定的适用范围，而组织在该范围内开展其运作。要实现合规，合规框架的范围必须直接参照前面已讨论的 GDPR 第 2 条中所描述的要求。

GDPR 适用于完全或部分以自动化的方式处理个人数据，以及以非

自动的方式处理已成为或计划成为档案系统一部分的个人数据。

也就是说，你的框架必须涵盖所有涉及个人数据收集、使用或其他处理（如删除或修改）的所有活动。对于许多组织来说，这几乎覆盖了他们的所有活动。请记住，这里并没有明确说明个人数据只是顾客的，你还必须把你的雇员、承包商等的个人数据考虑进来。

当然，也存在一些豁免，但这些豁免通常要么是涉及欧盟的高级别事务（例如成员国出于国家利益或欧盟安全而开展的活动），要么是针对主管当局开展刑事司法活动，要么就是涉及非常底层的活动（例如自然人在纯粹个人或家庭事务中所做的个人数据处理，而非那些以商业目的为诉求的、组织化的处理）。

属地范围

如前所述，GDPR 明确表示其[69]：

适用于不在欧盟境内设立的控制者或处理者对欧盟内数据主体的个人数据进行处理的有关情况：

（a）向欧盟内的数据主体提供商品或服务，不论该数据主体是否需要付费。

（b）对欧盟内数据主体发生在欧盟内的行为进行监测。

换句话说，世界上的任何组织，只要其向欧盟内的数据主体提供服务，都可能受制于 GDPR。请参考 GDPR 鉴于条款第 14 条中的描述："本条例保护其个人数据受到处理的自然人，不论其国籍或居住地是哪里。" GDPR 赋予所有数据主体相同的权利，无论他们居住在世界的哪个地方，只要其数据是由欧盟内的控制者或处理者处理的，或是由向欧盟提供服务的一方处理的。这可能会对隐私合规框架须考虑的范围有重大的影响。

此外，GDPR 还要求设在欧盟以外的组织以书面形式在欧盟内部指定一个组织作为其代表。[70] 该代表必须在目标数据主体所在的一个成员国设立，并且必须由数据控制者或处理者做出授权，在涉及个人数据处理的所有事务上对监管机构或数据主体做出响应。然而，任命这样一名

[69] GDPR，第 2（1）条。
[70] GDPR，第 3 条。

代表并不能使控制者或处理者规避因违反 GDPR 而带来的法律后果。

合规框架可能还需要考虑一些其他的因素，例如地方或部门特有的法律和条例。

治理

所有组织都有义务遵守法律，董事的信托责任之一就是确保其组织已采取适当的举措来实现守法。此外，董事还负有责任来确保组织所面对的风险得到妥善管理——很多时候体现为法律和合同义务。例如，网络风险（Cyber risk）就是董事必须意识到的一种风险类型。网络攻击会使组织的声誉和业务受到严重损害，由此遭受个人数据侵害的人也有可能寻求法律行动。GDPR 赋予了任何数据主体就处理其数据所造成的物质和非物质损害寻求司法救济的权利。这一点，连同 GDPR 对于数据泄露通报的具体要求，以及针对违规行为的严重行政处罚（最高可达全球年营业额的 4% 或 2000 万欧元，以数额较大者为准），都应成为所有董事关注的焦点，并列入各董事会会议的议程。董事会应确保已建立的隐私合规框架能够对 GDPR 合规，并且包含相应的机制向董事会定期提供关于整个组织合规情况的报告与保证。

在信息和隐私风险方面，董事会履行治理责任的一种方式是任命一名董事会级别的高级信息风险责任人（Senior Information Risk Owner，SIRO）。SIRO 的作用是从业务角度，而非技术角度来管理信息风险，并且聚焦在与实现企业目标相关的、战略性的信息风险上。这意味着组织要对其整个供应链上的信息风险通盘考虑，并根据组织的风险偏好对其进行管理。这对于董事会来说是一个有用的角色。而该角色应与董事会成员合作，以：

- 制定信息风险战略，既使资产得到开发，也能让风险得到有效管理；
- 识别对业务至关重要的信息资产，设立目标、优先次序及计划，以实现对信息这一业务资产的最大利用；
- 建立并维护恰当的风险偏好，以及对应的风险边界及容忍度。

显然，这一角色有比单纯管理隐私风险更大的责任。而现实是，任何管理隐私风险的框架，都必然是更大的信息风险管理框架的一部分。

因此，将解决 GDPR 的合规作为更大的信息风险管理战略的一部分是合理的。

这一治理要素应表现在对 GDPR 合规项目的必要资源承诺（人员、资金和系统方面）、最高管理层的领导和承诺（可被证明），以及公司的隐私政策与整个的内部沟通。

在 2013 年后发布的几乎所有 ISO 管理体系标准的第 5 条及其附加条款中，都包含了多项涉及最高管理层承诺的具体要求；这些要求为任一组织确立一个企业治理框架的领导地位提供了一个好的起点。第 5 条的要求如下：

最高管理层通过以下方式呈现其对管理体系的领导和承诺：

a. 确保政策和目标已制定，且与战略方向相一致；

b. 确保将管理体系融入组织过程；

c. 确保管理体系所需的资源是可用的；

d. 宣传有效管理和遵守管理体系要求的重要性；

e. 确保管理体系达到预期的效果；

f. 引导并支持有关人员促进管理体系的有效性；

g. 促进持续的改进；

h. 支持其他相关管理角色在其职责领域发挥领导作用。

ISO/IEC 38500:2015 是一个有关企业信息和通信技术治理的专门标准。它为创建一个有效的技术治理框架提供了有用的指导。

目标

隐私框架将涉及多个目标。总体目标显然应该是对 GDPR 合规，避免“劝诫性”罚款与其他惩罚措施。框架还应明确与数据主体权利及个人数据保护有关的具体附属目标。

目标应以能够被跟踪和衡量的方式来设立。毕竟，一个目标只有在判定它能真正达成时才有用。目标应当满足：

- 具体的；
- 可衡量的；
- 可采取行动（或可达到）的；
- 现实的；

·有期限的。

信息安全控制措施的实际表现要能够被衡量并改善，而 ISO/IEC 27004:2016 为衡量这些控制措施提供了具体的指引。虽然这一标准对衡量控制措施的表现来说是一个不错的起点，但它并不包含衡量特定数据隐私目标效能的指导。

其中关键目标包括：

·能够在新的规定时限（1 个月[71]）内对主体的查阅请求做出回应；

·有能力在 72 小时内发现数据泄露事件，并向监管机构报告；

·个人数据的保留期限；

·员工意识培训。

关键程序

隐私框架应该有一些关键性程序，其中的一些在你的组织中可能已经有了，而另一些则可能是新的。这些程序包括事故管理、变更管理、整改、风险管理和持续改进。

事故管理程序——本书第 14 章将作讨论——事关当发生数据泄露或其他信息安全事故时应该怎么做。

基本上事故管理程序将包括以下几个阶段：

1. 意识到发生了什么并报告；
2. 了解发生了什么；
3. 控制事件，以减少损失；
4. 修复损害；
5. 确保事件不会再次发生；
6. 检讨组织的响应。

事故管理流程的有关输出，将提示组织的框架应如何演变以适应其当前和未来的挑战。

组织还需要“变更管理”的程序。所有组织都必须对风险和有关事件做出改变和调适，并根据客户和市场的需求做出变化。当改变是以非结构化的方式做出时，可能会引入新的、不可预见的风险，涉及与信息和通信技术有关的进程尤其如此。对业务流程（或对部门、或对汇报结

[71] GDPR，第 12 条。

构）的变更管理不足，可能会对个人信息造成风险，并可能破坏现有的隐私保护机制。变更管理流程是一个重要的步骤，它可以确保变更是经过深思熟虑的，变更可能带来的偏差、问题和后果已被识别并得到缓解，且有相应的回撤方案。

整改程序也是必要的，这样的话，当某些事情未按预期的方式发展时，例如当控制不充分，资产未得到恰当保护，或一个更大的系统性错误导致整个流程失效，组织就可以进行补救。以上任何一种情况，组织都需要一种系统的方法来识别和纠正错误。

你可以在这里看到事故管理和变更管理程序之间的明显联系。一旦事故得到处理，就应对事故的原因进行分析，进而发现应对现有控制或程序所做的修正或变更。这些变更应通过整改程序来处理，确保整改能得到审查和批准，能被正确实施，且有效性得到审查。其中最后一点值得你注意：整改的行动需要对问题做出纠正，因此你的程序中还需要包括一个审查阶段，可能是一次性的审定，也可能是持续的关注——这是这一程序所要确认的。

其中一个更关键的程序是风险管理，本书第十一章将更深入地讨论这个问题。所有组织都面临风险，就 GDPR 合规而言，重点将放在个人数据的风险以及交互这些数据的系统和程序的风险上。

风险管理是任何隐私合规框架的核心，因为组织需要准确了解其需要保护自己免受什么风险，就像一个人可能会穿上一套盔甲来保护自己免受伤害，但这套盔甲对于有毒气体来说却完全无用，或者对于对抗一只熊来说可能效用有限。企业应确保将资金和资源投入正确的地方，因此建立一个有效的风险管理体制是确保其投入物有所值的好方法。

不过，就隐私风险而言，风险管理方案还必须密切关注处理自然人的数据可能对“自然人的权利和自由”造成的风险。从某种意义上说，GDPR 告诉了组织如果他们未能充分管理对数据主体造成的风险，就会面临巨额的行政罚款和数据主体付诸法律行动的风险。也就是说，组织的风险管理活动必须同时考虑到个人数据可能受到的风险，以及不合规对组织本身造成的风险。

一个框架或者管理体系还应该有一个持续的改进流程。一个持续改

进的流程会评估现有流程及其产出是否符合法律、条例或其他要求，确定任何必要的调整，然后将这些重新纳入初始的流程来确定框架或管理系统新的输入项。简单地说，你可能需要引用 PDCA 循环（Plan–Do–Check–Act，也称为戴明环），这是一个流行的过程模型，用于确保持续的改进。

其他持续改进循环，如 COBIT（Control Objectives for Information and Related Technologies）的持续改进生命周期或 ITIL（Information Technology Infrastructure Library）的持续服务改进过程，可以用来作为 PDCA 循环的替代。

PDCA 循环将管理体系或开发过程的标准过程和实践分为四个不同的阶段：计划、实施、检查和行动。作为一个循环过程，每一个阶段都会为下一个阶段提供反馈，从而实现持续的改进。

简而言之，组织应：

- 计划它将要做什么；
- 按照计划行事；
- 检查其工作是否达到预期目标；
- 根据所发现的问题采取行动，以改进其实现目标的方式。

PDCA 循环如图 2 所示。

理解其程序和针对这些程序的持续改进之间如何相辅相成，是实现

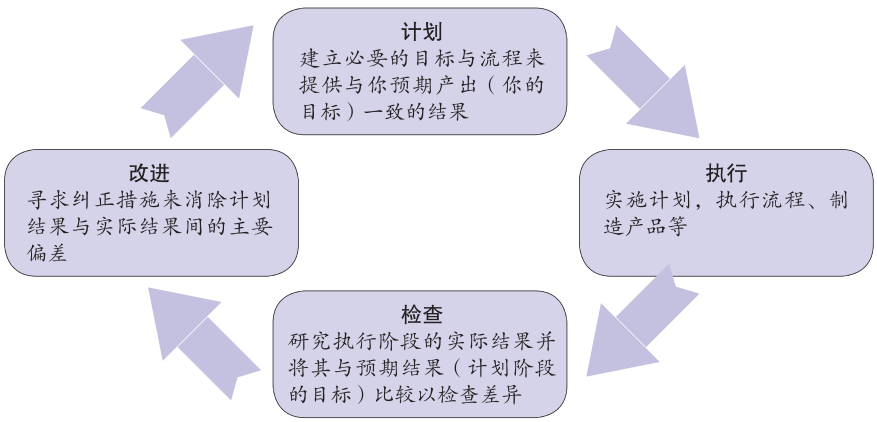

图 2 PDCA 循环

任何有效的合规框架的一个关键要素。假若你的所有程序都是合乎需要的，且都得到了遵循，那么这样框架就可以保证你能持续调整和改进你的流程，以便持续地满足你的合规要求。

个人信息管理系统

个人信息管理系统（PIMS）是一种用于管理个人信息的管理系统。因此，它可以构成一个合规框架的良好基础。

必须指出的是，尽管 PIMS 与合规框架大致相似，但二者是有区别的。例如，合规框架不一定只是“单个对象”，它可能由两个或两个以上的管理系统 [例如 PIMS 和信息安全管理系统（Information Security Management System，ISMS）] 共同协作而成。个人信息管理系统可能侧重于单纯地管理个人信息，但不一定按照法律或法规要求保护个人信息。从这个意义上讲，PIMS 可能只提供了确保总体合规所必需的一些程序。

虽然个人信息管理系统的设计不一定是为了确保符合 GDPR 或更具体的法律 [如英国的《数据保护法》（DPA）或德国的《联邦数据保护法》（BDSG）] 的具体规定，但标准化的模型通常会包括该项要求，即识别与个人信息有关的立法、监管和合同要求，并将这些要求纳入个人信息管理系统。

还有几种可能的方法来搭建此系统。《BS 10012:2017——数据保护——个人信息管理系统规范》就提供了一个这样的框架，它为数据保护管理提供了一个定义良好、易于理解的结构，并且遵循 PDCA 循环以确保持续改进。尽管该标准的早期版本是针对英国的《数据保护法》，但它已经被重新起草和更新，以体现 GDPR 的要求，因此，BS 10012:2017 总体上适合作为隐私合规框架的一个核心。

BS 10012 标准包括一项要求，即“确定个人管理信息系统的范围，并制定个人信息管理目标，同时适当考虑到……适用的法律、法规、合同和 / 或专业职责”。[72] 这意味着，要正确地运用 BS 10012 中所描述的程序，就应考虑到适用的法律要求。

然而，BS 10012 本身并非一个完备的框架，其适用性还取决于你的

[72] BS 10012:2017，第 4.3 条。

组织如何收集、储存和使用个人数据。BS 10012 仅限于隐私保护，如果个人数据被更广泛地应用于你的各业余流程，那么采用一个更全面的安全框架将是合适的。在这种情况下，可能需要定义额外的流程来保证合规。这就需要一个额外的管理体系，例如 ISO 27001。ISO 27001 作为一个国际标准，描述了一个信息安全管理系统的最佳实践要求。

如前所述，ISO 27001 可以通过应用 ISO 27701 来扩展，用以创建它所提到的隐私信息管理系统（也就是 PIMS）。ISO 27701 所遵循的模式并非专门针对 GDPR，而是旨在允许组织将其应用于与其有关的任何数据和隐私保护的要求。因此，尽管没有直接提及 GDPR，但它更加灵活——该标准提供了一个简单的映射来说明它在哪些方面应对了该条例的关键要求。

无论采用何种标准或业务流程模型，PIMS 都可能是你的隐私合规框架中的一个有用的内核。图 3 提供了对其典型组件的一个概述。

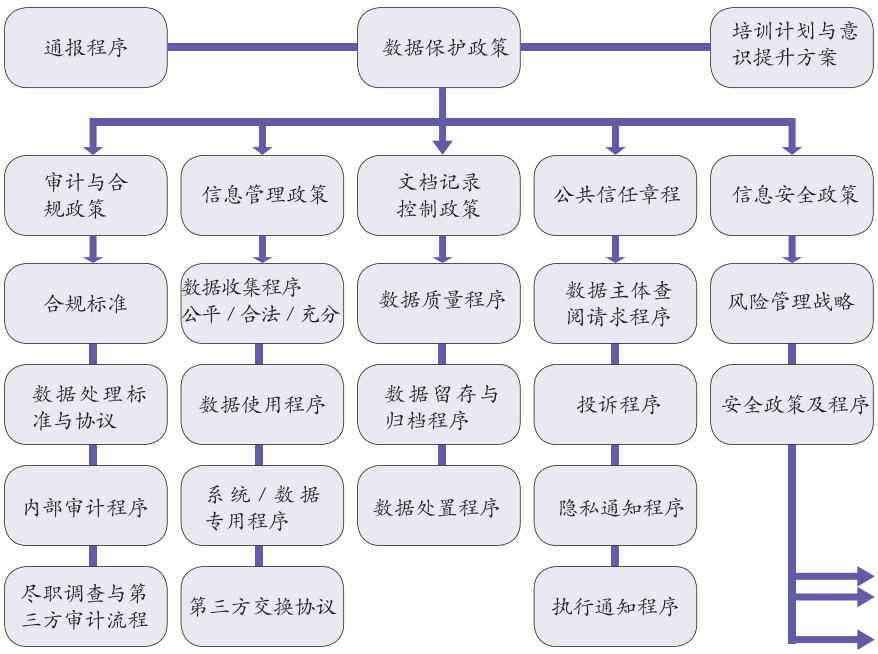

图 3 典型组件概述

ISO/IEC 27001:2013

GDPR 要求各组织采取更进一步的措施，而不仅仅是简单地建立一个 PIMS。GDPR 对各组织提出了明确的要求：

（a）有能力确保处理系统和服务有持续的保密性、完整性、可用性和可恢复性；

（b）在发生物理或技术事故时，有能力及时恢复个人数据的可用性与可访问性；

（c）有一个流程来定期测试、评估和评价技术与组织措施的成效，以确保处理的安全性。[73]

以上意味着，组织必须将数据和隐私保护纳入“日常业务”中，而有一个全面的信息安全方法来保障处理系统和服务，连同其安全性、连续性和持续的安全测试（主要以渗透测试的形式）至关重要。这就是 ISO 27001 的用武之地。

ISO 27001 本身与领域无关，且不偏向任何技术或解决方案，可供任何规模的组织使用。它规定了为保障信息安全你必须做些什么，但它同时也为组织结合其自身目标和风险偏好来落实这些要求留有一定余地。

这一信息安全框架也可以经由被认可的外部认证来做验证。这类认证所提供的保证被广泛承认可作为组织保护其信息资产的证明。在越来越多涉及有价值信息的合同中，相关的认证正成为一种要求。

在结构上，ISO 27001 与 BS 10012 没有太大的区别：两者都是由组织的高层驱动，描述那些对保护个人数据至关重要的流程，并认识到其作为更完整的结构中的一部分，还应另有一些流程来对这些流程进行管理。而两者的区别在于，BS 10012 专门关注个人信息，而 ISO 27001 关注的则是更广泛的信息。因此，一个基于 ISO 27001 的信息安全管理系统可作为一个更大的框架来纳入 BS 10012 。

图 4 显示了一个基于 ISO 27001 的信息安全管理系统架构。

· 机密性是“不向未经授权的个人、实体或程序提供或披露信息的

[73] GDPR，第 32（1）条。

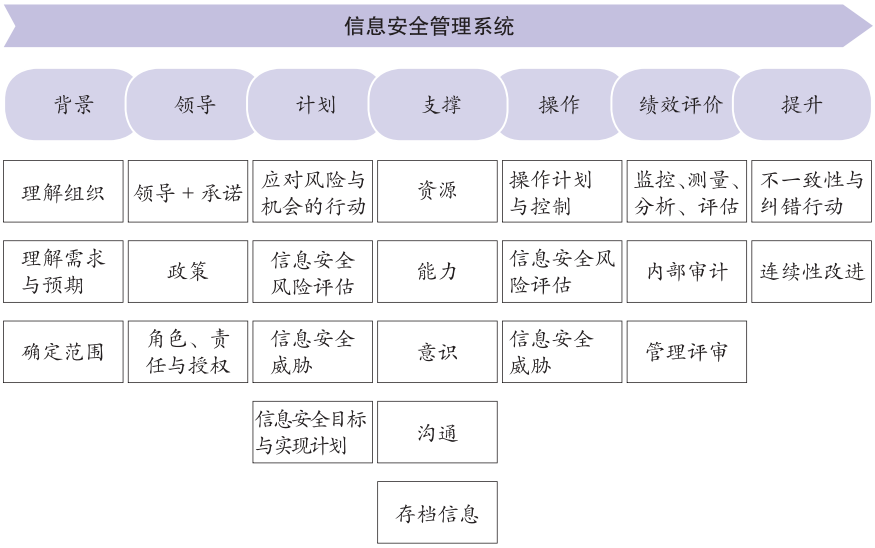

图 4 基于 ISO 27001 的信息安全管理系统构架

属性”[74]；

- 完整性是“准确性和完备性的属性”[75]；
- 可用性是“在一个授权实体要求下可访问和使用的属性”[76]；
- 风险是“不确定性对目标的影响”[77]。

因为机密性、完整性和可用性是安全信息的关键属性，它们通常被简称为信息安全的 CIA。GDPR 本身也多次提到了它们。同样，如你在本书的后面将看到的，ISO 27001 应对风险的方法与 GDPR 对影响评估的要求是一致的。

ISO 27001 采取了自上而下驱动信息安全的方法。因此，它涉及了这样一个要求：由最高管理层签署的信息安全政策，必须通过诸如风险管理、监控、审查、纠正等关键流程来落实。

ISO 27001 的附件列出了 14 个类别的 114 个控制项，这些可用于确定哪些是可以帮助管理个人信息安全的合适控制项。图 5 显示了这 14 个控件类别（注：图 5 中各空间类编号为 ISO 27001 标准的编号）。

[74] ISO/IEC/27000:2016，第 2.12 条。
[75] ISO/IEC/27000:2016，第 2.40 条。
[76] ISO/IEC/27000:2016，第 2.9 条。
[77] ISO/IEC/27000:2016，第 2.68 条。

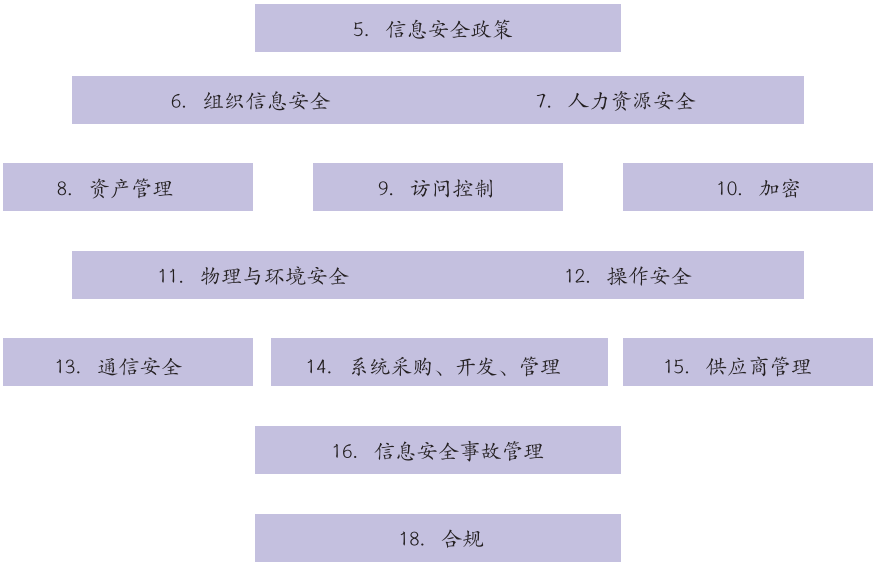

图 5 ISO 27001 附件中的 14 个控件类

在关于如何实施这些控制方面，艾伦·考尔德（Alan Calder）和史蒂夫·沃特金斯（Steve Watkins）的《IT 治理：数据安全国际指南与 ISO 27001/27002》[78] 提供了详细而实用的指导，目前已出第七版。而涉及如何设计和实施符合 ISO/IEC 27001:2013 标准的信息安全管理系统，可参阅艾伦·考尔德的《通往成功的九个步骤：ISO 27001 实施概览》[79] 或布里杰·凯尼恩（Bridget Kenyon）的《ISO 27001 控制——实施与审计指南》[80]。IT 治理要求国际委员会（International Board for IT Governance Qualifications，IBITGQ）也给出了实施和审计 ISO 27001 的有关规范。

实施 ISO 27001 标准的组织自然地会发现自己积累了遵守该标准的证据，尤其是当他们为其 ISMS 寻求外部认证时。这种证据的作用不仅仅是获得认证，或向客户展示你的流程是安全的，当一个组织受到调查或审计，它可以利用这些证据证明其一直在遵循最佳实践，采取了适当步骤以预防事故，正视了其所面临的风险，整个组织的各级人员都得到

[78] www.itgovernance.co.uk/shop/product/it-governance-aninternational-guide-to-data-security-and-iso27001iso27002-7thedition.
[79] www.itgovernancepublishing.co.uk/product/nine-steps-to-success.
[80] www.itgovernancepublishing.co.uk/product/iso-27001-controls-aguide-to-implementing-and-auditing.

适当的培训，是胜任且负责的。

其他标准

虽然 ISO 27001 和 BS 10012 是最有可能用作隐私合规框架基础的候选标准，但你也可以使用其他标准和业务流程模型。无论你选择哪一种，以及你是否选择这里提及的某个标准或业务流程，都取决于你的组织及其特定的流程、资源和要求。

COBIT 是一个基于控制的信息治理框架。它对于合规而言似乎是一个略为抽象的方法，但建立治理和监督机制，连同确立问责制和相应的责任，将是其一个重要组成部分来确保个人数据的安全和隐私。COBIT 是一些国家广泛使用的框架，特别是在企业层级，已有相应的出版物和可以在必要时提供咨询和指导的专家。

政府机构在面对复杂的立法时还制定了其他框架来简化合规的程序。虽然这些框架可能并不直接针对 GDPR 的合规，但它们往往包含一个有效的结构和程序来满足欧洲的合规要求。例如，澳大利亚信息专员办公室（Office of the Australian Information Commissioner，OAIC）所制定的《隐私管理框架》[81] 是一个符合 PDCA 循环的简单的四阶段规程，在其每个阶段都提供指导，以确保在澳大利亚的法律范围内合规，并遵守与澳大利亚有日常贸易的其他国家提出的其他相关要求。

美国国家标准与技术研究所（The US National Institute of Standards and Technology，NIST）也建立了一个信息安全标准的广泛集合，即 NIST 特殊出版物 800 系列。尽管它并不是一个专门的信息安全管理框架，但那些需要遵守联邦信息处理标准（Federal Information Processing Standard，FIPS）200 要求的美国政府机构就使用了 NIST SP 800-53 模型。虽然 NIST SP 800-53 可能主要是针对政府机构的，但这个框架肯定也可以应用到其他行业。然而，这是一个非常庞大的控制集，可能会让人无从应对。而 NIST SP 800-171 则是一种缩略的控制集，可推荐给没有保护联邦信息直接要求的组织使用。

NIST 网络安全框架为这两个控制集提供了有力的支撑，该框架提供了一个模型，以根据你的需求和成熟度方法来选择和实施有关的安全

[81] www.oaic.gov.au/agencies-and-organisations/guides/privacymanagement-framework.

控制。该框架还利用 NIST 控制集、ISO 27001 和其他框架来为特定的控制提供指导。虽然它并不直接解决隐私问题，但确实为此提供了一个可以进行适应性调整的有力基础。

选择与执行一个合规框架

是选择一个还是设计或编制一套特定的框架来保证合规？这一决定将基于一些关键考量。

首先，合规项目涉及的范围决定了该框架需要达到详细程度和覆盖的组织范围。这方面，你需要考虑多个因素，包括你的组织是数据控制者还是数据处理者、组织收集或处理个人数据的种类及数量、处理个人数据的端到端流程、收集及处理数据的不同方法等。分析这些信息以清晰地定义项目的范围是非常重要的一步，特别是当你选择使用了一个或多个管理系统标准（例如 PIMS）来开发你的合规框架时。

除了合规项目的范围，你的组织所收集、储存或处理的个人数据也会影响你对合规框架的选择。如果你处理的是特殊类别的个人信息，如健康信息，或者处理特别大量的数据，GDPR 需要你有额外的措施来确保数据的安全。因此，你的合规框架可能需要额外的流程来确保你符合这些要求，并且有足够的合规证据。

组织的复杂性也会影响你对合规框架的选择及其应用的范围。例如，对于一个流程众多的大型组织来说，没有必要让一个合规框架去干扰那些数据保护范围之外的流程。相反，一个组织如果因一系列职能上的不同目的而广泛使用个人数据，则需要一个框架来应对每一个业务目标下的数据处理。在某个流程中保护信息的方法很可能与另一个流程中的完全不兼容。

除了确保框架适合你的组织的具体需要，你还应该考虑你所在行业或领域的其他人使用的框架。这将帮助你思考其他组织已经确定的特定领域需求，并让你利用任何现有的经验或知识。

如前所述，许多组织在个人数据或信息方面还将受到一些其他的法律或监管要求，包括世界各地区不同的管辖要求，从信息自由的有关立法到 HIPAA 的数据可携性要求等等。在选择合规框架时应考虑到这些因素。有些法律和条例要求提供具体证据，以证明合规，这些证据与

GDPR 要求的可能有相当程度的重叠。

其次，你的组织在管理系统和框架方面的经验也会影响你的决定。对于没有这方面经验的组织，我们一般建议从已建立的标准开始，例如 BS 10012 和 ISO 27001，因为可用于支持你项目的特定标准已经很丰富。对于经验更丰富的组织来说，其选择可能会受到想通过对现有管理系统的扩展，将个人信息管理囊括进来的想法的影响。在这种情况下，你需要确保该组织的内部压力和既有流程不会干扰到项目的主要目标：有合适并相称的控制措施来保护个人数据，并能证明对 GDPR 的合规。

最后，资源的可用性、有无支持和指导也是重要的影响因素。再次强调，在合规或数据保护方面经验较少的组织，需要确保在组织内部和外部都有合适的资源，以确保项目可行。

框架实施

一旦你决定了你的隐私合规框架的起点，你就需要确定它应如何与你的组织整合。谁对每个流程负责？谁来监督？哪种培训是必要的？这类问题，结合 GDPR 的要求，将明确你应如何从核心要求开始来构建框架。

从首要的原则开始，合规框架应由组织正式的隐私和数据保护政策驱动，这些政策应公布并提供给合适的相关方，包括雇员。该政策需要明确组织在数据隐私和数据保护方面的立场，声明其致力于遵守 GDPR 和其他数据保护相关的法律法规，并由合适的最高管理层，如董事会或 CEO，签字批准。

在数据保护策略之下，你还需要定义并记录将该策略转化为实践的基本数据保护流程。你可以通过一套流程“地图”做到这一点。每一个具体的流程都应该被完整地记录，以便确定对其流程负责任的人，能通过一种提供一致结果的方式清楚地知道：必须做什么，由谁做什么，以及何时做。通常，这是通过一个 RACI 表来完成的。RACI 表为每个流程（或流程中的步骤）定义了谁是：

- 直接负责的；
- 承担责任的；
- 应被咨询的；

· 应被告知的。

绘制 RACI 表的目的是确保流程的设计和运作符合业务要求，始终如一地、可靠地执行，并与正式的要求保持一致，从而使管理层能够依靠它来达成所需成果的交付，见表 2。

表 2 绘制简单的表

流程	CEO	领导	领导	财务领导	法务	用户
A	R+A	C	I		C	I
B		C	R+A		C	
C		C	R+A		C	I
D		I		A	R	I
E	C	I		I	R+A	I

你需要通过流程的输出物和活动记录来确认：你是否遵守了法律，以及你的框架是否符合组织的要求。因此，你需要考虑哪些是能提供这些信息的考核指标，以及你该如何收集这些信息。有些指标可能只是简单地记录某一流程执行的次数，而另一些则可能是基于对员工的调查。

制定一个合规的监控方案是这一方法的合理延伸，它涉及通过实施一个合规测试流程来监控你的系统或框架。有许多方法可以衡量管理系统或框架的有效性，与该主题相关的书众多。这一评估过程将为你的持续改进提供参考，包括发现你的组织什么时候未能遵守规定，并努力加以修正；或是看到一个未发挥其作用的流程，然后做出改进。

整改和持续改进的流程在前文已做讨论。这种不断的改进对于保证你遵守 GDPR 是必要的。随着业务流程、策略和控制手段的演变，你的框架也必须随之改变。