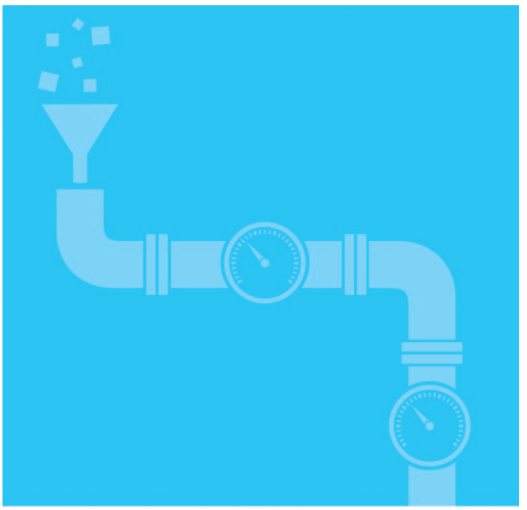
第一章
持续审计

第 1 节　持续审计简介

阅读指南

本节介绍“持续审计”这一章的目的、定位和结构。

一、目标

本章的目标是讲述持续审计的基本知识以及应用持续万物这一领域的技巧和窍门。

二、定位

持续审计是持续万物概念的一个方面。本章包含了持续实施合规性的各种技术，这些技术可以在开发过程中不断提高信息系统的质量。“持续”一词指的是采用增量和迭代的方式开发软件，形成一个代码流，并通过 CI/CD 安全流水线持续过渡到生产环境。这个代码流就如同一条价值流，需要不断优化。

持续审计是一种敏捷方法，我们可以在设计信息系统的过程中定义它的行为、功能和质量，用来实现所需要的控制，从而减轻或消除已识别的风险。持续审计与 DevOps 8 字环的所有方面有直接或间接的关系，因为它是整体设计的。这意味着持续审计涵盖了信息系统（技术）、生产过程（流程）以及知识和技能（人员）等多个方面。因此，持续审计提供 PPT（People, Process, Technology，人员、流程和技术）层面的设计。

信息系统的设计是确保系统控制安全的重要基础。近年来，许多组织质疑信息系统的设计。将信息系统的信息捆绑起来并让所有利益相关方参与进来的传统做法被敏捷的工作方式和三人组开发策略视为已经过时的理念。这个做法意味着要从业务、开发和测试三个方面提前考虑一个要构建的增量，这样就能更好地解决“怎么做”和“做什么”的问题，并能就增量的完成定义（Definition of Done, DoD）达成共识。但是，这忽略了设计另一个重要的功能：控制功能。该功能旨在通过实施适当的对策来防止因缺乏措施而导致的风险，包括但不限于违反法律和监管义务的风险。信息安全也是至关重要的控制要素，它涵盖信息的保密性、完整性和可用性。

从持续审计角度来看，DevOps 领域的发展至关重要。目前，一些组织仍在采用瀑布式项目的工作方式，这种工作方式需要进行大量的设计工作；而另一些组织则发现仅仅使用用户故事并不是最佳方案，某种形式的设计仍然是必要的。因此，系统开发领域再次趋于平衡，为持续审计提供了坚实的基础。

当然，问题在于是否所有类型的信息系统都应该采用同样的工作结构。随着 Gartner 的商业智能（Business Intelligence, BI）模型的出现，区分记录型系统（System

of Records, SoR）和交互型系统（System of Engagement, SoE）变得至关重要。除了SoE，现在人们还谈论智能型系统（System of Intelligence, SoI）。图 1.1.1 概述了这三种类型的信息系统（SoR、SoE 和 SoI）之间的关系。

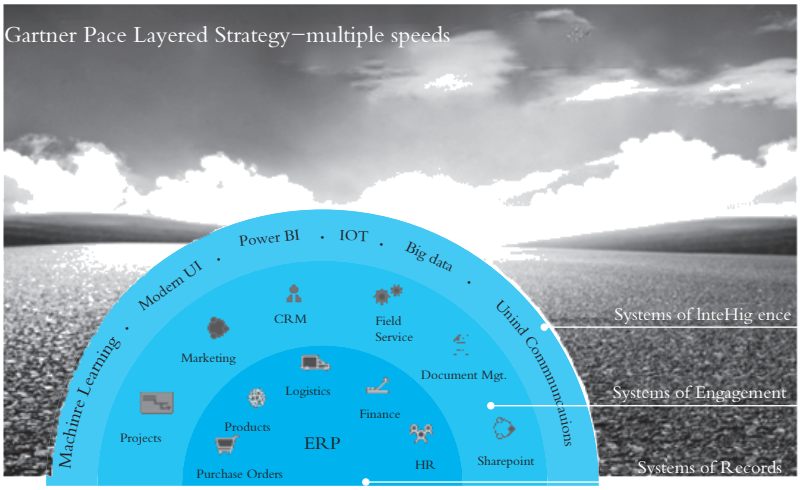


图 1.1.1　SoR、SoE 和 SoI

（来源：结果公司 HSO）

（1）SoR

SoR 是后台办公室的信息系统，完成财务、物流、库存和人力资源管理（Human Resource Management, HRM）任务。这些系统由政府监管，必须满足多种法律和监管要求，例如税务机关、荷兰中央银行（De Nederlandse Bank, DNB）和荷兰金融市场管理局（Anthority for the Financial Markets, AFM）的规定。此外，《萨班斯 - 奥克斯利法案》（*Sarbanes Oxley*, SoX）和《通用数据保护条例》（*General Data Protection Regulation*, GDPR）也是证明信息系统设计合法化的依据。

财务信息系统还必须满足会计师的要求，以便在年度账户获得签名。这意味着，除了其他事项外，还需要设计方案来表明财务数据是如何产生的，以及不同相关信息系统的接口是什么。这些系统通常是信息系统链的一部分，需要经过深思熟虑，因此合规性在设计中发挥着重要作用。

（2）SoE

销售渠道，特别是网络商店和智能手机应用程序，是面向消费者的 SoE 的主要目标。这些应用程序可以轻松地提供新版本、补丁和更新。这些信息系统通常不是信息系统链的组成部分，而是链条的终点。在敏捷开发和运维一体化（DevOps）的相关出版物中，它们也经常被用作案例。对于这些信息系统而言，显然事先经过考虑的设计（前置设计）是不太必要的，通常它们可以用成长式设计（新兴设计）来满足需求。

然而，实践证明对于这些 SoE 来说，仅仅具有一系列用户故事是不够的。更重要的是，用户故事通常会被放置在迭代的待办事项列表中，并在迭代完成后进行归档。这会导致单独的用户故事并不能形成对信息系统的可访问描述。因此，仍然需要一

种能够提供对系统功能、质量和运行状况的概览和洞察的设计方案。尤其重要的是，用户界面和数据源接口是安全和持续审计的重要方面。

（3）SoI

除了上述系统，还存在BI解决方案，具体指各种报告、数据分析工具等。与SoE类似，BI能基于SoR的信息进行呈现，并且更易于修改。然而，数据泄露始终是一项潜在风险。风险的高低取决于所提供信息的价值。因此，必须准确评估信息风险并采取相应的防范措施。

（4）持续审计的必要性

对于三种类型的信息系统（SoR、SoE和SoI），都需要一定程度的控制，因此我们需要进行持续审计。

单靠一组用户故事并不能全面了解和监控信息系统所承受的控制要求，也难以及时、准确地识别出适应和扩展信息系统所带来的风险和影响。然而，必须避免风险应对措施（控制）的实施破坏生产过程的敏捷性。这意味着，不仅控制的设计和监控要增量迭代地进行（持续审计），而且控制也必须基于加权风险进行选择，控制措施既不能太多，也不能太少。控制设计定义的程度可随信息系统类型而变化，从SoR的详细定义到SoE的精简定义，再到SoI的近乎无定义。即使对于SoR，控制设计也可以分为前置定义（提前）和新兴出现（迭代）的两个层面。

三、结构

本章介绍了如何使用持续审计金字塔模型来塑造持续审计。在讨论该模型之前，首先将讨论持续审计的基本概念和基本术语、定义、基石和架构。接下来的几节所介绍的内容是对该模型的讨论。

1. 基本概念和基本术语

本书的这部分阐述了持续审计涉及的基本概念和基本术语。

2. 持续审计定义

有一个关于持续审计的共同定义是很重要的。因此，本书的这部分界定了这个概念，并讨论了信息系统设计和管理不当所造成的潜在问题及其成因。

3. 持续审计基石

本书的这部分讨论了如何通过变更模式来定位持续审计，在此我们将得到以下问题的答案：

- 持续审计的愿景是什么（愿景）？
- 职责和权限是什么（权力）？
- 如何应用持续审计（组织）？
- 需要哪些人员和资源（资源）？

4. 持续审计架构

本书的这部分介绍了持续审计的架构原则和模型。架构模型包括持续审计金字塔模

型和持续控制模型。

5. 持续审计设计

持续审计的设计定义了持续审计价值流和用例图。

6. 持续审计最佳实践

本书的这部分介绍了如何构建控制框架，并讨论了一些持续审计最佳实践。

7. 持续审计实施

第 8、9、10 节（持续审计概念、CA 工具设计、持续审计实施）讨论了如何将持续审计应用于实际操作。

第 2 节　基本概念和基本术语

提要

- 持续审计是根据实现控制的 6 个步骤进行讨论的。
- 通过使用分层的持续审计金字塔模型，审计可以提供逐步的风险消除和缓解。
- 持续审计金字塔中的层结构可以用来分配持续审计的所有权。

阅读指南

本节在讨论持续审计的概念之前，首先定义基本概念和基本术语。

一、基本概念

本部分介绍了两个与持续审计有关的基本概念，即持续审计金字塔和持续控制，这两个概念通过一系列将在下一部分定义的术语进行描述。

1. 持续审计金字塔

本书的这部分强调了基于 6 个步骤的持续审计概念：

（1）确定范围（目标运营模式）

（2）选择目标

（3）识别风险

（4）设计并实施控制措施

（5）建立并适时调整对控制措施的监控

（6）评估控制措施的有效性

图 1.2.1 以持续审计金字塔的形式对这些步骤进行了概述。金字塔各层宽度体现了执行该步骤所需的精力。在这里，“做什么”这个问题会逐渐演变为“怎么做”的问题，这正如史蒂夫·乔布斯（Steven Jobs）的著名言论：“设计这个词很有意思。一些人认为设计指的是外观，但是，如果你深挖这个概念，会发现它指的是产品是如何运作的。”这句话也适用于持续审计金字塔的设计。

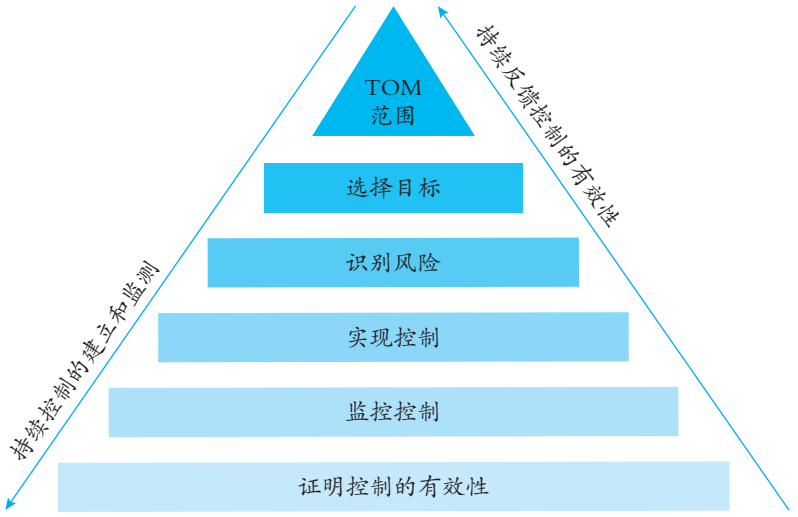


图 1.2.1　持续审计金字塔

2. 持续控制

图 1.2.2 展示了持续控制模型。从该模型可以看出，必须根据已确定的风险（风险转化）将目标转化为控制措施。我们应该使用短期（领先监控）的测量来衡量控制的有效性。如果发现偏差，可以收集更多的测量数据来强化控制措施。

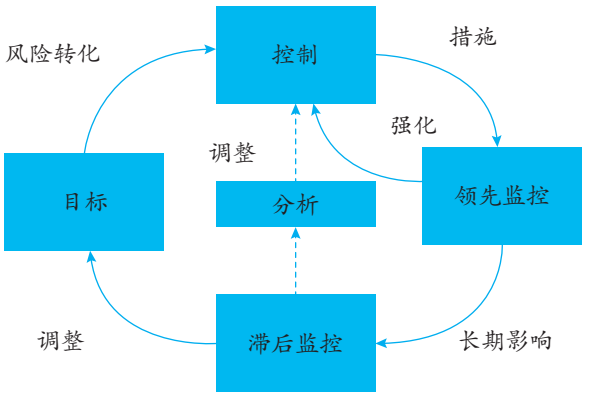


图 1.2.2　持续控制模型

为了观察长期效应，短期测量数据将被汇总（滞后监控）。若目标被证实不切实际，可进行相应调整。对汇总后测量数据的分析亦可能导向控制的调整。

二、基本术语

本部分定义了与持续审计相关的基本术语，并首先讨论了持续审计金字塔的步骤。

1. 持续审计金字塔

（1）确定范围

目标运营模式（Target Operating Model, TOM）是理想的方案，也被称为未来状态（Soll）。TOM 的目标是提高财务价值和社会价值。该方法通过迁移路径（Migration path）逆转当前状态（Ist）以实现未来状态。Ist–Soll– 迁移路径建模通常是架构师基于组织的使命、愿景和战略定义而设计的。一旦使命、愿景或战略发生变化，通常也需要调整 TOM。TOM 由一个或多个价值链组成，每个价值链又包含多个价值流。在过去的 30 年中，TOM 的信息规划已经从 5 年加速到 1 年甚至更短，它的变异率仍是相对较低的。持续审计的范围是在 TOM 内根据选定的价值流，特别是那些产生最大成果增长的价值流来选择的。

（2）选择目标

为了监控战略的实现和成果的增长，我们需要设定目标。这些目标通常是通过平衡计分卡等可视化工具来制定。如今，精益指标也越来越多地用于监控成果改进。最终，每个目标都必须以增长成果为目的。然而，一些不可控因素（外部影响因素）作为成果增长的前提条件，也需要被纳入目标设定中。例如，GDPR 立法和 ISAE 3402 标准就属于这类因素。由于强制性的法律法规，它们也必须被纳入目标设定过程。

组织也可以选择遵循某个标准来更好地吸引客户，例如 ISO 27001:2013 标准，它表明信息安全符合独立定义的标准。

（3）识别风险

任何目标的达成都存在一定风险。这些风险可能性质各异，并高度取决于设定的目标。

（4）确定控制措施

面对风险，我们可以选择承担或者控制，但不应该忽视它。承担风险意味着不采取任何措施，任由风险发生；而控制风险则必须采取应对措施来消除或减轻（降低概率或影响）风险。衡量标准的选择取决于组织的风险偏好（愿意承担多少风险）和雄心壮志（愿意为了达到目标承担多少工作量）。

（5）确定监控措施

风险管理的有效性应通过衡量控制措施的运作情况来确定。

（6）确定证据

控制的有效性需要通过客观证据来确认。这种证据必须由独立方客观地获取，并用来向利益相关方证明控制能够在多大程度上保护目标。

2. 价值链

1985 年，迈克尔 • 波特（Michael Porter）在其著作《竞争优势：创造和维持卓越绩效》（1998 年版）中提出了价值链的概念，见图 1.2.3。

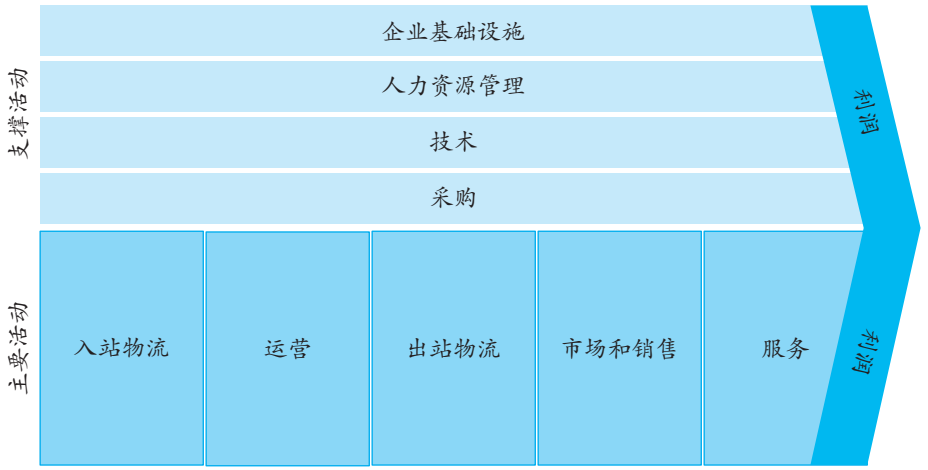


图 1.2.3　波特的价值链

（来源：《竞争优势：创造和维持卓越绩效》，1998 年版）

波特认为，一个组织通过一系列具有战略意义的活动为客户创造价值，这些活动从左到右看就像一条链条，随着链条的延伸，组织及其利益相关方的价值创造也不断增加。波特认为，一个组织的竞争优势源于它在其价值链活动的一个或多个方面做出的战略选择。

该价值链与下一小节描述的价值流模型具有几个显著的不同之处。这些差异主要体现在以下方面：

- 价值链被用来支持企业战略决策。因此，它的应用范围是总体的公司层面。
- 价值链展示了生产链中哪些环节创造了价值，哪些环节没有。价值从左到右增加，每个环节都依赖于之前的环节（链条左侧）。
- 价值链是线性的、操作性的，旨在体现价值的累积过程，并不适用于流程建模。

3. 价值流

价值流概念并没有明确的来源。但许多组织已经在不知不觉中应用了这一概念，例如丰田汽车的丰田生产系统（Toyota Production System, TPS）。价值流是一种可视化流程的工具，描述了组织内一系列增加价值的活动。它是按时间顺序排列的商品、服务或信息流，逐步增加累积价值。

尽管价值流在概念上与价值链类似，但也有重要区别。我们可以通过以下方面进行对比：

- 价值链是一个决策支持工具，而价值流则提供了更细致的流程可视化。在价值链的某一环节，如图 1.2.3 中的 “服务”，可以识别出多个价值流。
- 与价值链一样，价值流是商业活动的线性表述，在不同的层面上发挥作用。原则上不允许分叉和循环，但对此没有严格的规定。
- 价值流经常使用精益指标，例如前置时间、生产时间和完成度 / 准确度，但这在价值链层面并不常见。不过这并不排除为价值链设定目标的可能性。将平衡计分卡层层分解到价值链和价值流是合理的。
- 与价值链不同，价值流可以识别具有多个步骤的分阶段生产过程。

4. DVS、SVS 和 ISVS

在 ITIL 4 中，定义了服务价值体系（Service Value System, SVS），为服务组织提供了实质性内容。SVS 的核心是服务价值链。SVS 可放置在图 1.2.3 中 “技术”层的支持活动。这是整个波特价值链的递归。这意味着价值链的所有部分都以服务价值链的形式复制到 SVS 中，如图 1.2.4 所示。

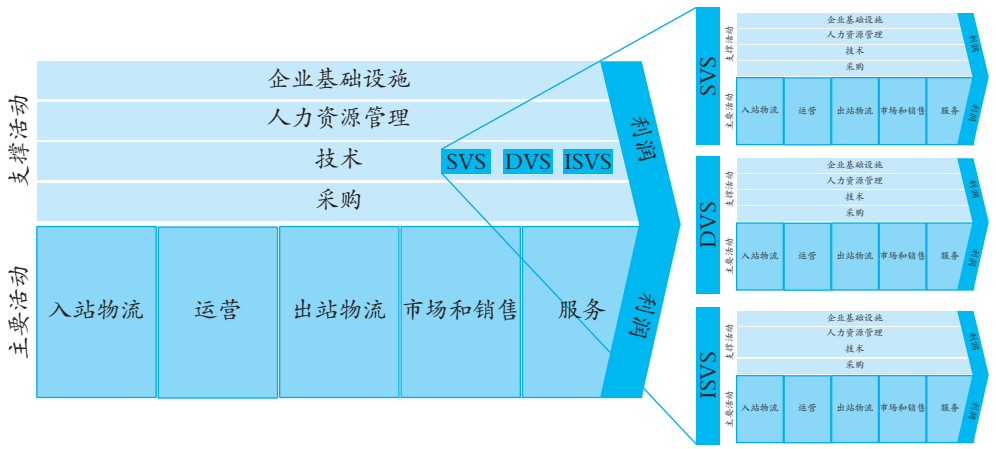


图 1.2.4　波特的递归价值链

（来源：《竞争优势：创造和维持卓越绩效》，1998 年版）

这种递归并不是新概念，因为在《信息系统管理》（2011 年版）中已将其视为递归原则。业务流程（R）被递归地描述为管理流程。类似于 SVS，信息安全价值体系（Information Security Value System, ISVS），即 ISO 27001:2013 中定义的信息安全管理体系（Information Security Management Sytem, ISMS），也可以被视为波特价值链的递归。这同样适用于定义系统开发价值流的开发价值体系（Development Value System, DVS）。

另一种递归可视化如图 1.2.5 所示。

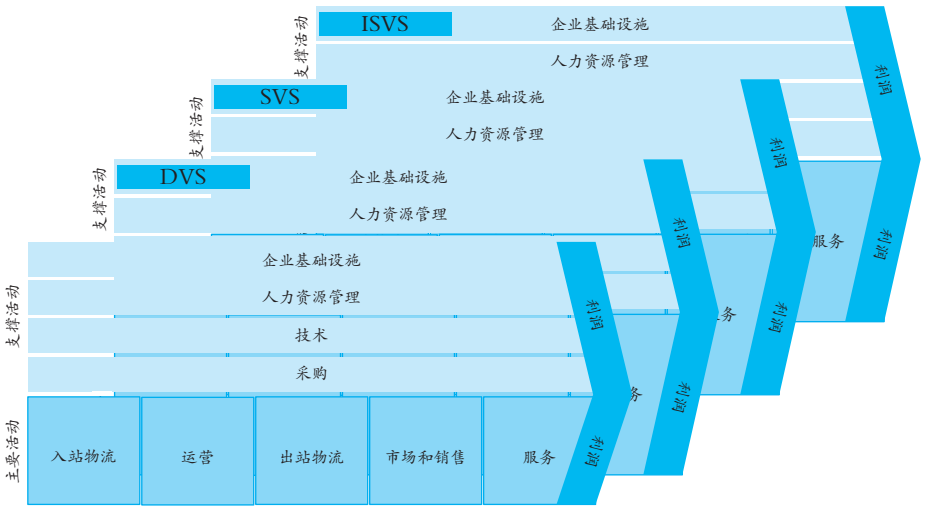


图 1.2.5　另一种波特的递归价值链

（来源：《竞争优势：创造和维持卓越绩效》，1998 年版）

两种可视化的区别是，图 1.2.5 假设价值链具有波特结构，而 ITIL 4 中定义的 SVS 没有波特结构。因此将价值链定义为图 1.2.4 所示则更为合适。

作为 ITIL 4 SVS 核心的服务价值链有一个运营模型，用作指示价值流的活动框架。服务价值链模型是静态的，只有当价值流贯穿其中、共同创造和交付价值时，才会产生价值。

5. 持续审计定位

图 1.2.4 表明，在波特价值链中可以识别出若干价值体系，即 SVS、DVS 和 ISVS。图 1.2.6 表明，这 3 个价值体系由原则、实践、治理、持续改进和价值链组成。

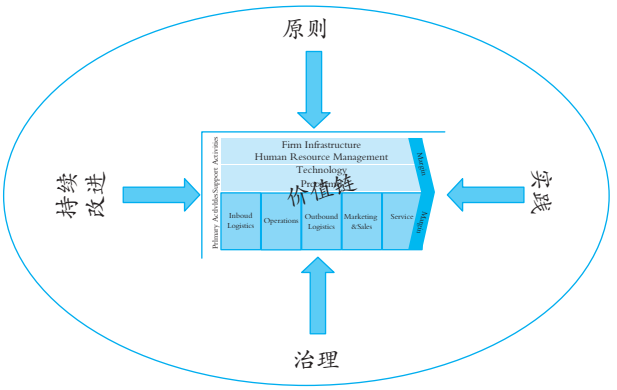


图 1.2.6　价值体系的构建

原则上，价值链是波特价值链的一种应用，如图 1.2.3 所示，价值链的目的体现了其应用。

对于 SVS 来说，这是运维层面的 TOM 设计；对于 DVS 来说，这是开发层面的 TOM 设计；而对于 ISVS 来说，这是信息安全层面的 TOM 设计。

价值链由价值流组成，价值流由价值系统提供的实践组成。例如，ITIL 4 提供了构建 SVS 价值流的管理实践，而 ISO 27002:2013 则为 ISVS 的价值流提供了最佳实践，《持续万物》（2022 年版 ）一书提供了 DVS 和 SVS 的 DevOps 实践。

图 1.2.7 示意性地展示了业务价值链的结构。

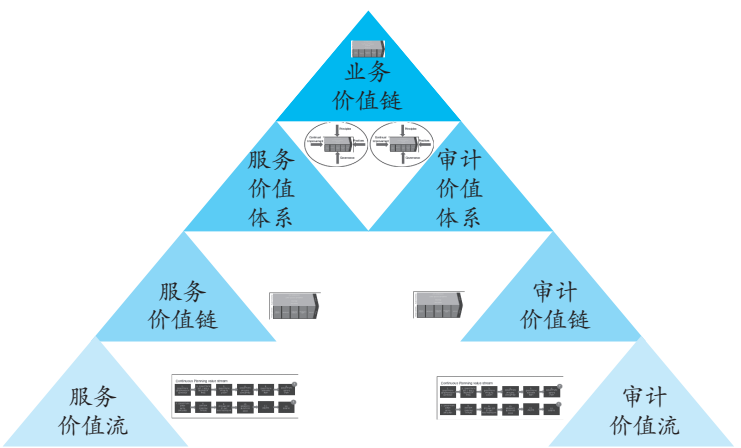


图 1.2.7　业务价值链的构建

对于持续审计，如今有各种各样的控制保障措施可供选择。其中一种方法是定义一套新的审计价值体系（Audit Value System, AVS）。在此基础上，可以细化构成审计价值流的原则、实践、治理、持续改进和审计价值链。另一种方法是将控制纳入相关的价值体系，即 SVS、DVS 和 ISVS。

由于 AVS 基于持续审计金字塔，其控制纯粹聚焦于审计，从而提升了控制的重要性，因此优先推荐使用这种方法。此外，由于信息安全是持续审计的一个重要方面，我们还可以选择将 ISVS 与 AVS 集成。本书的这一部分为设计 AVS 提供了基础。

第 3 节　持续审计定义

提要

- 持续审计应被视为一种持续风险管理方式，通过持续审计可以创造价值。然而，需要正确的认知才能识别和理解这种成果的增长。
- “审计”一词带有负面含义，但审计就像一面镜子，让我们看到可以做得更好的地方。
- 为了保证创造价值，持续审计必须被看作是消除和减轻风险的整体方法。

阅读指南

本节介绍了持续审计的背景和定义，然后基于特征性问题概述了经常发生的问题，并分析了持续审计提供解决方案的根本原因。

一、背景

持续审计的目的必须是保证业务成果的增长。具体而言，它通过更快地向利益相关方反馈信息，帮助它们了解所识别的风险的应对措施在信息系统的行为、功能和信息质量方面是否能有效实现。提升业务成果的实际衡量标准通常在于信息安全领域的风险管理以及遵守法律法规，例如财务报告和个人数据处理的相关规定。这些方面是企业在制定 TOM 及其目标时所期望的成果的前提条件。

二、定义

本节对持续审计的定义如下。

> 持续审计是针对一个包含人员、流程、合作伙伴和技术的价值链，持续进行全面评估，确保其处于受控状态。
> 这通过持续监控控制的设计、存在和运作的有效性，并利用反馈信息改进控制来实现。
> 控制是针对无法实现质量目标的风险所采取的应对措施。质量目标源于价值链的目标运营目标。

三、应用

持续万物的每个应用都必须基于业务案例。为此，本节描述了信息系统持续控制方面的典型问题，这些问题隐含地构成了使用持续审计的业务案例。

1. 有待解决的问题

需要解决的问题及其解释见表 1.3.1。

表 1.3.1　处理持续审计时的常见问题

P#	问题	解释
P1	传统的审计公司由于多种原因面临着新技术的挑战，审计人员在开展信息安全认证时，对新技术的考虑尚不充分	主要原因包括： • 敏捷开发方法下，高频率的小规模变更并非总是经过控制措施有效性测试 • 信息系统、云服务之间的接口或云服务之间的接口是灵活且变化迅速的 • 希望持续保持控制的公司不能证明它们的 IT 环境符合法规或暴露出了漏洞，这意味着无法立即知晓控制措施的有效性，只能在审计期间确认
P2	反馈缓慢	ICT 领域的变化越来越频繁，而年度审计只能给人在一年后才得到控制的印象
P3	控制措施难以理解	没有记录控制措施的设计、存在和运作，难以证明合规性
P4	没有可追踪性	从收集到的证据中无法明确该数据是针对哪个目标收集的
P5	没有信息系统设计	如果应用程序的设计不是以价值流、用例图、用例或类似形式进行的话，则无法正确确定隐含风险的保障
P6	没有风险管理	在风险登记册中没有记录风险，也没有记录在风险发生时采取的措施
P7	没有监控功能	监控设施不是针对控制信息系统的
P8	没有证据	没有证据表明该信息系统符合适用的法律和法规，该组织无法向客户证明其处于控制状态
P9	风险被忽略	由于风险偏好过高，为了达到目标而承担的工作量过少，缺乏控制或有意识地承担风险的能力

2.根本原因

找出问题的原因的久经考验的方法是 5 个“为什么”。例如，如果不存在（完全）持续审计方法，则可以确定以下 5 个“为什么”。

（1）为什么我们没有实施持续审计?

因为没有人要求始终保持控制。

（2）为什么没有必要始终保持控制?

因为审计有负面的含义，被视为浪费，持续审计更是如此。

（3）为什么持续审计被视为浪费?

因为风险管理被认为非常耗时，会影响新功能的快速交付。

（4）为什么持续审计被视为耗时的?

因为没有价值体系（例如 ISVS）或价值流（例如信息安全价值流），无法保证控制措施与信息系统共同设计，导致需要进行重构才能构建控制措施或手动监控控制措施。

（5）为什么没有价值系统或价值流专门用于控制？

因为管理层的风险偏好过高或为了达到目标而承担的工作量过少，这也可能取决于

组织的成熟度或者组织高层的管理能力不足等，还有更多的原因可以列举。总的来说，总会有一种潜在的意识，这种意识通常被日常问题中确定的目标而不是质量目标所控制。通常情况下，如果整个组织因软件劫持事件而瘫痪，或所有公司机密被泄露到互联网上，或因竞争对手获得了所有客户和员工数据而陷入困境，那么组织更愿意投资于控制措施。

这种树形结构的 5 个“为什么”问题使我们有可能找到问题的根源。必须先解决根源问题，才能解决表面问题。因此，在没有资金进行改革或进行后续培训的情况下，我们开始评估是没有意义的。

第 4 节　持续审计基石

提要

- 持续审计的应用需要自上而下的驱动和自下而上的实施。
- 通过持续审计确定的控制结构的管理，可以通过制定路线图来优化，将改进点纳入技术负债的待办事项列表中进行有序处理。
- 持续审计的设计应从一个能够表达其必要性的愿景开始。
- 对持续审计的有用性和必要性达成共识十分重要，这可以避免在设计过程中产生过多争论，并为统一的工作方法奠定基础。
- 变更模式不仅有助于建立共同愿景，而且有助于引入持续审计金字塔并遵循这一方法。
- 如果没有设计权力平衡步骤，就无法开始实施持续审计的最佳实践（组织设计）。
- 持续审计强化了一个追求快速反馈的左移组织的形成。
- 每个组织都必须为持续审计的变更模式提供实质性的内容。

阅读指南

本节首先讨论可以应用于实现 DevOps 持续审计的变更模式。该变更模式包括 4 个步骤，从反映持续审计愿景和实施持续审计的业务案例开始，然后阐述权力平衡，其中既要关注持续审计的所有权，也要关注任务、职责和权限；接下来是组织和资源两个步骤，组织是实现持续审计的最佳实践，资源用于描述人员和工具方面。

一、变更模式

图 1.4.1 所示的变更模式为结构化设计持续审计提供了指导，从持续审计所需实现的愿景入手，可防止我们在毫无意义的争论中浪费时间。

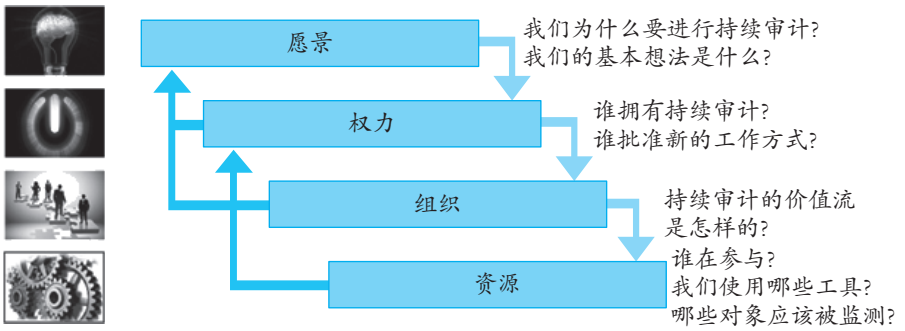


图 1.4.1　变更模式

在此基础上，我们可以确定权力关系层面的责任和权限划分。这听起来似乎是一个老生常谈的词，不适合 DevOps 的世界，但是猴王现象（Monkey Rock Phenomenon，猴王现象可以指代人们盲目地模仿他人的行为、观点或习惯，而不考虑其真实的价值或合理性）也适用于现代世界，这就是记录权力平衡的重要性所在。随后，工作方式（Way of Working,WoW）才能得到细化和落实，最终明确资源和人员的配置。

图 1.4.1 右侧的箭头表示持续审计的理想设计路径。左侧的箭头表示在箭头所在的层发生争议时回溯到的层级。因此，有关应该使用何种工具（资源）的讨论不应该在这一层进行，而应该作为一个问题提交给持续审计的所有者。如果对如何设计持续审计价值流存在分歧，则应重提持续审计的愿景。以下各部分将详细讨论这些层级的内容。

二、愿景

图 1.4.2 展示了持续审计的变更模式的步骤图解。图中左侧部分（我们想要什么？）列出了实施持续审计的愿景所包含的各个方面，以避免发生图中右侧部分的负面现象（我们不想要什么？）。也就是说，图中右侧的部分是持续审计的反模式。下面是与愿景相关的持续审计指导原则。

我们想要什么?	我们不想要什么?
1.我们想要有效控制 我们希望控制措施能对保证结果的增加做出有效的贡献。	1. 临时性的控制措施 2. 迟来的反馈信息 3. 瀑布式的实施 4. 可追溯性方面的缺陷
2.我们希望得到快速反馈 我们希望在自动监测控制的基础上获得快速反馈。	
3.我们想要一个增长模型 我们希望有一个实施控制的路线图。	
4.我们想要可追溯性 我们想要从证据到目标的可追溯性。	
指导原则： P1−1.控制是有效的。 P1−2.持续审计应有助于快速反馈。 P1−3.获得并保持控制是一个增长过程。 P1−4.获得的每一个证据都可以追溯到一个目标。	

图 1.4.2　变更模式——愿景