

设计和实施	设计方法	从战略到系统架构	组织必须从业务战略开始，使用该战略制定更具体的目标。然后从每个目标派生出详细的业务需求。组织需要与架构设计人员合作，将这些业务需求转换为构成信息系统架构的系统要求、标准和流程的更详细视图
		从系统架构到系统设计	将信息系统架构转换为系统设计时，需要继承信息系统架构并添加更多细节，包括实际的硬件、数据、网络 and 软件
	架构模式	转换框架	转换框架将业务战略转化为信息系统架构进而转变为信息系统设计，转换框架提出了三类问题：内容、人员和位置，需要为每个信息系统组件回答这些问题
		集中式架构	集中式架构下所有内容采用集中建设、支持和管理的模式，其主体系统通常部署于数据中心，以消除管理物理分离的基础设施带来的困难
		分布式架构	硬件、软件、网络 and 数据的部署方式是在多台小型计算机、服务器和设备之间分配处理能力和应用功能，这些设施严重依赖于网络将它们连接在一起
		面向服务的架构（SOA）	SOA 架构中使用的软件通常被引向软件即服务（Software-as-a-Service, SaaS）的相关架构，同时，这些应用程序在通过互联网交付时也被称为 Web 服务



优化和持续改进	定义阶段	待优化信息系统定义	该活动关注定义协同的范围、优化目标和目的、系统团队成员和出资人，以及优化时间表和交付成果
		核心流程定义	该活动关注定义利益干系人、投入和产出以及广泛的功能
		团队组建	该活动重点关注从关键利益干系人群体中确定人员组建高能力团队，对信息系统的问题和收益达成共识
	度量阶段	流程定义	流程定义通常使用流程图工具定义度量阶段的流程，以图形方式实现给定信息系统的输入、操作和输出
		指标定义	待优化信息系统的定义包括将用于评估流程的指标
		流程基线	当明确了度量指标之后，必须通过基线确定现有系统的能力，以确定当前系统在多大程度上较好地满足了服务对象的要求，并验证定义阶段中确立的信息系统目标达成情况
		度量系统分析	度量是根据某些规则将数值分配给被观察到的现象。在对信息系统进行优化和持续改进过程中，需要十分注意度量水平、度量的可靠性与有效性问题
		价值流分析	价值流分析首先定义信息系统使用者眼中相关产品或服务价值
	分析阶段	信息系统异常的源头分析	度量阶段的信息系统异常的来源，提供了信息系统稳定(即控制中) 或不稳定 (即失控) 的证据
		确定优化改进的驱动因素	优化改进的驱动因素是指对信息系统优化影响最大的因素
	改进 / 设计阶段	改进/设计的解决方案推进	改进/设计阶段解决方案的部署可以缩小信息系统当前状态与所需状态之间的差距
		定义新的操作 /设计条件	定义阶段中引入的核心流程可用于开发新流程，还可以进行其他实验设计，以确定新信息系统或新系统中新的功能和设计所需的最佳操作条件，以最大或最小化响应
		定义和缓解故障模式	建立了信息系统的优化和持续改进流程之后，可以评估其故障模式
	控制/ 验证阶段	标准化新程序/新系统功能的操作控制要素	当信息系统得到改进，组织需要更好地控制系统，保持进一步改进的能力
		持续验证优化的信息系统的可交付成果	组织应当将变更的系统组件信息、信息系统状态趋势等内容，对受影响的人员开展培训
		记录经验教训	随着项目小组完成其活动，必须最终确定和保留项目文档。其中一个关键方面是记录经验教训，如为了更快或更好的结果，可能会做些什么事情

信息系统管理


数据战略	数据战略规划	数据战略规划是在组织所有利益相关者之间达成共识的结果
	数据战略实施	数据战略实施是组织完成数据战略规划后，逐渐实现数据职能框架的过程
	数据战略评估	组织在数据战略评估过程中需要建立对应的业务案例和投资模型，并在整个数据战略实施过程中跟踪进度，同时做好记录供审计和评估使用
	数据治理组织	数据治理组织需要包括组织架构、岗位设置、团队建设、数据责任等内容，它是各项数据职能工作开展的基础
	数据制度建设	为保障数据管理和数据应用各项功能的规范化运行，组织需要建立对应的制度体系
	数据治理沟通	数据治理沟通旨在确保组织内全部利益相关者都能及时了解相关策略、标准、流程、角色、职责、计划的最新情况，开展数据管理和应用相关的培训，掌握数据管理相关的知识和技能
	数据模型	数据模型是使用结构化的语言将收集到的组织业务运行、管理和决策中使用的数据进行综合分析，按照模型设计规范将需求重新组织
	数据分布	数据分布职能域是针对组织级数据模型中数据的定义，明确数据在系统、组织和流程等方面的分布关系，定义数据类型，明确权威数据源，为数据相关工作提供参考和规范
数据架构	数据集成与共享	数据集成与共享职能域是建立起组织内各应用系统、各部门之间的集成共享机制，通过组织内部数据集成共享相关制度、标准、技术等方面的管理，促进组织内部数据的互联互通
	元数据管理	元数据管理是关于元数据的创建、存储、整合与控制等一整套流程的集合
数据应用	数据分析	数据分析是对组织各项经营管理活动提供数据决策支持而进行的组织内外部数据分析或挖掘建模，以及对应成果的交付运营、评估推广等活动
	数据开放共享	数据开放共享是指按照统一的管理策略对组织内容的数据进行有选择的对外开放，同时按照管理策略引入外部数据供组织内部使用
	数据服务	数据服务是通过对组织内外部数据的统一加工和分析，结合公众、行业和组织的需要，以数据分析结果的形式对外提供跨领域、跨行业的数据服务

数据管理	数据安全	数据安全策略	数据安全策略是数据安全的核心内容，在制定的过程中需要结合组织管理需求、监管需求以及相关标准等统一制定
		数据安全标准	数据安全标准是数据安全策略的支撑，是数据安全策略的具体化，是数据安全策略的落地，是数据安全策略的支撑
		数据安全管理体系	数据安全管理体系是在数据安全标准与策略的指导下，通过对数据访问的授权、分类分级的控制、监控数据的访问等进行数据安全的管理工作，满足数据安全的业务需要和监管需求，实现组织内部对数据生存周期的数据安全管理
		数据安全审计	数据安全审计是一项控制活动，负责定期分析、验证、讨论、改进数据安全管理相关的策略、标准和活动
	数据质量	数据质量需求	数据质量需求是明确数据质量目标，并根据业务需求及数据要求制定用来衡量数据质量的规则，包括衡量数据质量的技术指标、业务指标以及相应的校验规则与方法
		数据质量检查	数据质量检查是根据数据质量规则中的有关技术指标和业务指标、校验规则与方法对组织的数据质量情况进行实时监控，从而发现数据质量问题，并向数据管理人员进行反馈
		数据质量分析	数据质量分析是对数据质量检查过程中发现的数据质量问题及相关信息进行分析，找出影响数据质量的原因，并定义数据质量问题的优先级，作为数据质量提升的参考依据
		数据质量提升	数据质量提升是对数据质量分析的结果，制定、实施数据质量改进方案，包括错误数据更正、业务流程优化、应用系统问题修复等，并制定数据质量问题预防方案，确保数据质量改进的成果得到有效保持
	数据标准	业务术语	业务术语是组织中业务概念的描述，包括中文名称、英文名称、术语定义等内容
		参考数据和主数据	参考数据和主数据是用于将其他数据进行分类的数据
		数据元	通过对组织中核心数据元的标准化，可以使数据的拥有者和使用者对数据有一致的理解
		指标数据	指标数据是组织在经营分析过程中衡量某一个目标或事物的数据，一般由指标名称、时间和数值等组成，指标数据管理指组织对内部经营分析所需要的指标数据进行统一规范化定义、采集和应用，用于提升统计分析的数据质量

2.管理要点

数据生存周期	数据需求	数据需求是指组织对业务运营、经营分析和战略决策过程中产生和使用数据的分类、含义、分布和流转的描述
	数据设计和开发	数据设计和开发是指设计、实施数据解决方案，提供数据应用，持续满足组织的数据需求的过程
	数据运维	数据运维是指数据平台及相关数据服务建设完成上线投入运营后，对数据采集、数据处理、数据存储等过程的日常运行及其维护过程，保证数据平台及数据服务的正常运行，为数据应用提供持续可用的数据内容
	数据退役	数据退役是对历史数据的管理，根据法律法规、业务、技术等方面需求,对历史数据的保留和销毁，执行历史数据的归档、迁移和销毁工作，确保组织对历史数据的管理符合外部监管机构和内部业务用户的需求，而非仅满足信息技术需求
理论框架与成熟度	数据管理能力成熟度模型	
	初始级	数据需求的管理主要是在项目级体现，没有统一的管理流程，主要是被动式管理
	受管理级	组织意识到数据是资产，根据管理策略的要求制定了管理流程，指定了相关人员进行初步管理
	稳健级	数据已被当做实现组织绩效目标的重要资产，在组织层面制定了系列的标准化管理流程，促进数据管理的规范化
	量化管理级	数据被认为是获取竞争优势的重要资源，数据管理的效率能量化分析和监控
	优化级	数据被认为是组织生存和发展的基础，相关管理流程能实时优化，能在行业内进行最佳实践分享
	数据治理框架	国际数据治理协会发布了 DGI 数据治理框架，是组织在进行数据治理的操作层面的框架体系，为组织做出决策和采取行动的复杂活动提供的方法
	数据管理能力评价模型	提供了用于建立和评估组织数据管理计划的关键维度，主要强调团队协作 (流程)、标准执行和资金支持
数据管理模型		国际数据管理协会 DAMA 在 2018 年发行了 DAMA-DMBOK (数据管理知识体系指南) 第 2 版，用于指导组织的数据管理职能和数据战略的评估工作，并建议和指导刚起步的组织去实施和提升数据管理

运维管理	能力模型	能力建设	组织需要考虑环境的内外部因素，在治理要求的指导下，根据服务场景，识别服务能力需求，围绕人员、过程、技术、资源能力四要素，策划、实施、检查和改进运行维护能力体系，向各种服务场景赋能，通过服务提供实现服务价值；并针对能力建设、人员、过程、技术、资源建立关键指标；还需要定期评价运行维护服务能力成熟度，衡量能力水平差距，以持续提升运行维护服务能力
		人员能力	组织人员能力建设聚焦在从知识、技能和经验维度选择合适的人，从人员管理和岗位职责维度明确做适合的事，目的是指导 IT 运维团队根据岗位职责和管理要求“选人做事”
		资源能力	资源主要由人员、过程和技术要素中被固化下来的能力转化而成，人员、过程和技术要素在知识、服务管理、工具支撑等方面的能力被固化下来，同时又对人员、过程和技术要素提供有力的支撑和保障，进而形成资源能力中的知识库、服务台、备件库以及运行维护工具，资源能力确保 IT 运维能“保障做事”
		技术能力	组织需要通过自有核心技术的研发和非自有核心技术的学习，持续提升 IT 运维过程中发现问题和解决问题的能力，在提升 IT 运维效率方面是重点考虑的要素，技术要素确保 IT 运维能“高效做事”
		过程	过程又称流程，是为达到特定的价值目标而由不同的人分别共同完成的一系列活动。 组织通过过程的制定，把人员、技术和资源要素以过程为主线串接在一起，用于指导 IT 运维人员按约定的方式和方法，确保 IT 运维能“正确做事”
	智能运维	中国电子工业标准化技术协会发布的团体标准 T/CESA 1172《信息技术服务 智能运维 通用要求》，给出了智能运维能力框架，包括组织治理、智能特征、智能运维场景实现、能力域和能力要素，其中能力要素是构建智能运维能力的基础	

<div> 信息安全管理</div>	CIA 三要素	CIA 三要素是保密性 (Confidentiality)、完整性 (Integrity) 和可用性 (Availability) 三个词的缩写		
	信息安全管理	在组织机构中应建立安全管理机构，不同安全等级的安全管理机构逐步建立自己的信息系统安全组织机构管理体系，参考步骤包括：1. 配备安全管理人员；2. 建立安全职能部门；3. 成立安全领导小组。		
	安全保护等级划分	第一级，等级保护对象受到破坏后，会对相关公民、法人和其他组织的合法权益造成损害，但不危害国家安全、社会秩序和公共利益		
		第二级，等级保护对象受到破坏后，会对相关公民、法人和其他组织的合法权益产生严重损害或特别严重损害，或者对社会秩序和公共利益造成危害，但不危害国家安全		
		第三级，等级保护对象受到破坏后，会对社会秩序和公共利益造成严重危害，或者对国家安全造成危害		
		第四级，等级保护对象受到破坏后，会对社会秩序和公共利益造成特别严重危害，或者对国家安全造成严重危害		
		第五级，等级保护对象受到破坏后，会对国家安全造成特别严重危害		

网络安全等级保护	<p>第一级安全保护能力：应能够防护免受来自个人的、拥有很少资源的威胁源发起的恶意攻击、一般的自然灾害，以及其他相当危害程度的威胁所造成的关键资源损害，在自身遭到损害后，能够恢复部分功能</p>
	<p>第二级安全保护能力：应能够防护免受来自外部小型组织的、拥有少量资源的威胁源发起的恶意攻击、一般的自然灾害，以及其他相当危害程度的威胁所造成的重要资源损害，能够发现重要的安全漏洞和处置安全事件，在自身遭到损害后，能够在一段时间内恢复部分功能</p>
	<p>第三级安全保护能力：应能够在统一安全策略下防护免受来自外部有组织的团体、拥有较为丰富资源的威胁源发起的恶意攻击、较为严重的自然灾害，以及其他相当程度的威胁所造成的主要资源损害，能够及时发现、监测攻击行为和处置安全事件，在自身遭到损害后，能够较快恢复绝大部分功能</p>
	<p>第四级安全保护能力：应能够在统一安全策略下防护免受来自国家级别的、敌对组织的、拥有丰富资源的威胁源发起的恶意攻击、严重的自然灾害，以及其他相当危害程度的威胁所造成的资源损害，能够及时发现、监测发现攻击行为和安全事件，在自身遭到损害后，能够迅速恢复所有功能</p>
	<p>第五级安全保护能力：访问验证保护级</p>

安全保护能力等级划分