项目风险管理：SAP实施项目中的风险控制和安全管理 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/457/2021_2022__E9_A1_B9_E7_9B_AE_E9_A3_8E_E9_c41_457849.htm 随着公司治理、内部控制（例如目前谈“ 萨 ”色变的萨班斯法案以及上海深圳证券交易所出台的《上市公司内部控制指引》）越来越多地被中国企业所接受并应用，信息安全和风险控制在企业信息系统实施项目中（如SAP实施项目）正扮演着越来越重要的角色。 作为全球领先的ERP软件，SAP正在为越来越多的大中型企业所使用，并使企业的整个价值链实现高度自动化。SAP可全面覆盖企业的业务运作和财务处理，乃至提供丰富的决策支持功能。同时，SAP也提供了全面、灵活的功能/模块来强化企业的内部控制，使企业的所有操作均可运作在一个高效且可控的应用平台上。正是因为SAP的庞大与复杂，如何实现相关的安全控制及数据安全往往是企业所面临的一个巨大挑战。 SAP系统控制和安全的实施不是简单地随着项目进行就能够自然而然地在系统里实现，这些都需要具有一定专业技能的控制和安全团队通过风险评估以及设计一定的控制框架来完成。SAP系统控制和安全的实施也是企业实现IT治理、内部控制和信息安全的必要的手段。评估企业是否采取足够的IT控制方法来减少业务流程风险也是控制和安全团队的一项重要任务。在SAP实施过程中，权限控制、系统配置、职责分离设置、数据校验以及监控报告都是可以采取的IT控制方法。 许多中国企业已经开始在SAP实施项目中使用独立的控制和安全团队致力于对系统安全的设计和实现。为了有效地进行SAP系统控制和安全的实施，我们将从三

个方面，也就是项目管理、技术管理及利益方（Stakeholder）管理三方面加以阐述。 一、项目管理 ---------- 符合利益方的期望 有效的对安全和风险控制进行项目管理就是要站在利益方的立场上考虑问题。控制和安全团队负责人必须清晰了解利益方重要的信息安全和控制需求。因此，对重要的利益方从内部业务流程控制方面进行访谈从而了解到哪些是企业需要保护的信息不失为一个直接的方法。控制和安全团队需要保证制定的安全策略和方法来体现企业目前IT和业务方面的变化。同样的，控制和安全团队也需要很好地和业务流程实施小组进行紧密地合作。 由于企业内部业务流程和对于信息安全的优先度考虑不一，不同的利益方对于SAP信息控制和安全有着不同的期望。了解利益方的业务需求会让控制和安全团队很好地了解项目的复杂程度以及安全实施的范围，并因此有益于对控制安全设计的时间和工作量的估计。 SAP信息控制和安全，作为业务流程控制的“ 代言人 ”，使得了解业务流程成为了控制和安全团队的必修课。举个例子来说，一个企业为了防止舞弊，设计了业务流程使得同一个用户不能同时创建以及批准采购订单，接收入库单，付款，以及维护供应商主档。为了实现这样的业务流程，控制和安全团队就需要设计权限来限制这些互斥的业务操作来达到职责分离。对一些小的企业来说，做到尽善尽美的职责分离由于公司人数过少而变得不可能，在这种情况下，控制和安全团队就需要设计一些补偿性控制（Compensating Control）来减少职责过于集中所带来的风险。比如说，控制和安全团队需要在SAP系统中考虑设置一定的“ 门槛值 ”，一旦超过这个“ 门槛 ”，相关的管理层就需要在用户进行业务操作前进行一

定的批准及授权。职责分离在内部控制监管制度，尤其是萨班斯法案中对管理层和审计师来说都是焦点之所在。 取得高级管理层和业务所有者（一般而言是那些业务经理）的认同和支持是安全和风险控制项目管理的另一个主要的方面。同高级管理层就SAP信息安全策略和方法进行探讨并取得他们的认同对于建立整个SAP项目团队的接受度，所有权和责任感都是至为关键的。 二、技术管理 ----------实现系统中的内部控制 在项目团队中拥有既了解内部控制监管环境，又深谙与SAP相关的系统控制设置的技术骨干是必不可少的。不过，在实际的SAP实施项目中，绝大多数的信息安全部门，尤其是SAP的控制和安全团队，经常是缺少必要的人员而且工作量以及工作难度都被过低地估计了。控制和安全团队在项目中往往被忽略，或者甚至由不了解内部控制的技术人员代替进行权限的设置以及安全策略的撰写。这样的直接结果就是SAP系统内的控制设置不足或不符合业务流程需要，用户权限过大而且职责没有完全分离等等。当系统上线，企业管理层再发现SAP内部控制问题之后，再想重新改正，一来“劳民伤财”，二来“积重难返”，很难通过内部和外部的审计。可见，拥有合适的系统安全人员对于SAP项目实施质量控制会有多大的作用。在项目过程中，控制和安全团队也须经常同企业内部审计部门就安全策略和方法进行沟通并进行一定的文档撰写和安全测试。 当控制和安全团队同利益方谈论SAP权限如何实现以及可选的安全控制方案时，控制和安全团队必须确保利益方不仅了解可能的权限限制的结果，而且明白如果没有设定必要的权限限制所带来的风险以及对企业内部控制的影响。另外，职责分离分析可以基于SAP角

色(Role)基础上。职责分离分析可以帮助企业确定，分析并列举用户访问企业敏感区域的权限，并且提供互相冲突的业务。许多SAP职责分离工具已经被开发出来用以自动地对SAP角色以及用户权限进行分析来提高效率并减少企业成本。国际上较为流行的SAP职责分离工具包括Virsa及Approva等，一些企业咨询公司如德勤开发的专有工具eQSmart也能够很好地进行职责分离分析。 三、利益方管理 ---------- 沟通带来成功 项目实施过程中管理好利益方，尤其是业务用户经常是SAP安全有效实施中最重要但无疑也是最复杂的一环。如果控制和安全团队不能和业务团队，技术人员以及管理层不能有效进行沟通的话，控制和安全团队也不可能获得所有的业务需求，更不可能将这些业务需求“ 翻译"成安全技术语言在系统内加以实现。如果这样的话，实施的效果就要打上一个很大的折扣，更不要提IT治理、内部控制和信息安全了。 从用户的立场上来看，控制和安全有时感觉像捆住了他们的手脚，权限的限制使得他们不能“ 为所欲为 ”地对系统功能进行访问、修改和操作，这不难理解。但从内控的立场上来看，安全控制就是保证系统访问的安全，不能让用户“ 为所欲为 ”。内控和用户对系统的方便使用一直以来都是一个相互制衡的话题，更多的控制当然会限制用户对系统的方便使用，但对系统过于方便的使用则不利于内控的实现。这就要求控制和安全团队能够从实际的业务需求出发，和业务团队和管理层进行很好的沟通，以达到用户对内部控制更多的理解并从实际工作中就注重提高安全和控制的意识。 SAP实施项目对每个企业来说都是一个综合的庞大工程，加强项目中安全控制，防范于未然，才能使企业在面临竞争时不会“ 千里之堤，

毁于蚁穴”，才能决胜于千里之外。 100Test 下载频道开通，各类考试题目直接下载。详细请访问 www.100test.com