项目风险管理：IT风险管理框架研究 PDF转换可能丢失图片或格式，建议阅读原文 https://www.100test.com/kao_ti2020/260/2021_2022__E9_A1_B9_E7_9B_AE_E9_A3_8E_E9_c41_260137.htm 风险管理是一个比较时髦的词，我们都在讲企业的风险管理，包括赖老师讲的SOX法，实际上就是控制企业的风险，引用一些控制措施，其中里面的控制措施里就有一个非常重要的内容就是IT的，IT如何去控制风险，IT如何为企业的风险做出应用的贡献，实际上这就是我们要研究的内容。实际上也是我们很多信息化管理者正在思考的问题，是到底是从哪里下手去做这个事情，这个事情的题目是一个很大的题目，到底从如何下手，那么我就结何我的实际经验和一些我研究的内容给大家做一些介绍。 首先给大家介绍一下我国信息化的现状，那么我国信息化是这样从78年到现在大概也就二三十年的时间，力度比较大的信息化建设，那么到今天为止实际上我们已经基本走过了一个基本的阶段，我们以前的信息化是什么呢，注重了对行业的覆盖，对企业的覆盖，硬件的配置等等，把什么建起来，把应用的系统建起来，那么从2000年开始，我们把重点就开始转移了，我们慢慢转移到信息化见效了，要做出贡献了，为业务解决问题了，为业务创造价值了，这是我我们更多的关注的内容。 至于用什么产品，虽然也很重要，但是已经让位给了IT如何为社会为政府创造价值就这么一个层面上来了，那么这个时候去讲究什么呢，讲究IT如何提供服务，如何控制他的风险，如何更好的来创造更多的本身的价值在里面，这个时候我们更多关注是IT本身更多的风险，这是为什么呢？打个比方，今天我们用电用水一样，政府和

企业不可分割的一部分，我们可能平时感觉不到，但是一但没有的话你就会感觉到你可能会受不了，你的企业可能就会停止运转，政府也可能会受影响，所以这种依赖性比较高的风险迫使我们去考虑如何控制IT，如何支持我们企业的组织、社会IT正常的运维。 从这几十年的IT实践来看，IT的风险其实很大，我们回过头来看，我总结了几条，实际上还远远不只是这些，这里面是几个比较重要的，比如IT治理的风险，刚才赖老师也提到IT治理的风险，我们现在很少提到这个词，但其实是件很重要的事，还有规划和架构的风险，我们也讲规划，但是我们这个规划与真正的标准化的可操作性的规划还是有一定的距离，我们还有项目管理风险，技术设施风险，应用系统风险，应用交互风险，信息安全风险，业务持续风险，IT绩效风险等等，我想随着时间的发展，还会有新的风险还会层出不穷的。 那么我简单分析一下这里面几个比较重要的风险： 第一IT治理风险，这几年的发展，我们发现我们国内的信息规划特别是我们就看看搞的特别好的企业，我们讲有几大模式，我们讲的斯达造纸厂IT信息化做的特别好，讲巩义电子政务做的好，我们看这些做的好的企业和政府有一个很重要的原因是什么，他的一把手特别重视，他的主要领导特别重视，一个比较懂行，别外一个可能是善于利用社会资源，领导重视做的比较好，有的单位可能做的不太好也有很多原因可能就是把IT当技术去处理了，我们讲实际上这个“ 人治 ”的时代，还没有到法制没有到一个真正治理的阶段，还要靠真的领导去认识那他就做的好。 对我们现在的这个社会来讲，靠人治是远远不够的，不能满足要求的，一定把他变成制度化的东西，不管是换了哪些领导，我们

的这个企业还是要往前发展的，那么我们的IT应该是什么样，就是什么样，不因为领导重视不重视而忽略或受到重视，在这个层面上我们国家目前都还基本在人治的层面上，没有建设成这么一个治理的概念。信息化是一个从治理层的关注，把它变成一个制度，需要有一个制度化，规范化，标准化，这里要涉及到许多机制，我们IT不光是技术的问题，实际上还有很多战略问题，管理、业务流程实践都要涵盖在里面，真正把这个制度建立起来，IT才会摆脱现在的状况。这是第一点，也是我们感受比较深的。 第二个就是规划和架构的风险，我们每个企业实际上政府在做信息化的时候都在做规划，五年规划，三年规划，我们的网络建设规划，应用规划，但好多规划实际上做的层面还是不够具体的，还不够标准化，操作起来还有许多误区在里面，王仰富先生会给规划这方面的内容，他讲的是一种国际上比较流行操作的一种手段，怎么去进行规划，而不是我们现在做的方式，这个问题我不展开讲。 下面谈项目管理风险，IT最终去实践，如果规划好了一个架构出来，如何去实践就变成一个项目，项目周期很长，比如去开发一个ERP软件，这个项目需要很长时间，这个风险就非常大，这么长的一个软件项目投资那么大，如果这个项目控制不好，风险非常大，这里面有几个统计数字，就是在美国信息化这么发达的国家，他的成功率也不是很高。我们国家呢，大家可能感受到这个就更不用说了，项目控制项目的审计，项目的监理，我们有一些有效的控制手段，但是这里面风险依然很大。 还有基础设施的风险，大家都知道现在的网络是越来越复杂，补丁露洞越来越多，开发层度越来越深，但是风险越来越高。这是为什么呢？因为系统

越来越复杂，这是一个非常自然的、信息化固有的风险。另外一方面我们对这个IT设施依赖性特别强，我们是不可忍受的，有人做过统计银行对IT的依赖最多不超过两天，证券公司网络停机不能超过半个小时，半个小时以上就是事故了。商企企业，实际上我们对他的依赖性是很强的，不能容忍任何的失误，经济发展的更新化越来越快，基础设施上的风险依然在加大。另一个风险是应用系统的风险，想到风险把目标放在安全上，实际上我们应用软件应用系统在开发过程当中，充满着风险，就是比如需求是不是清楚呀，我们现在开发出的软件不是我们想要的东西，因为经常是搞技术的人弄来一些人，在那做调研，软件开发公司来公司做调查，弄很多人在开发软件，搞软件的人不太懂业务，懂业务的人不太弄技术，有很大的脱节在里面，这只是一个风险。实际上还有一个风险就是我们在做软件开发的时候，很少把安全的控制做在软件的本身里面，举个例子去年的时候发生在日本的一个证券公司叫瑞穗证券，他是接受委脱人的指令操盘，进行证券买卖，结果他在接受指令的时候，操盘员敲错了，本来应该是一股61万日元一股，结果他敲反了，造成很大的损失，几分钟证券公司损失了270亿日元，相当于16亿人民币，大家都在说这个操盘员臭手，实际上我们作为风险管理人员审视这件事发现不是那个人手臭，你去操作你可能某一天也会出错，他实际上是一种控制的趋势，特别在应用开发方面上，很显然的错误没有在业务方面加强控制在软件上表现出来，这是一个巨大的缺陷，软件开发商不会主动的去给你业务部门搞这个事，太麻烦了，如果你自己不提，但是我们业务部门又很少提这样的风险上的要求，我们很多软件开发有

这样的趋势在里面，除了供用需求以外，我们将来还需要功能需要，软件开发功能需求加在一起做出软件开发的需求。还有就是IT服务交互风险，我的IT有露洞了，补丁包该打的都打了，服务器又特别好，那也不能百分之百的说你的IT好，实际上对用户来讲他关注的是服务，不管你用的是什么数据库还是什么的服务器，我们更多的关注的是这服务器性能好不好，一定要把IT的硬件软件要变成一个服务，为客户服务，这个理念也要在我们的IT中体现出来。 信息安全风险这个大家都比较明白，我们现在这个安全这块形势越来越严峻，安全方这面比如讲的病毒呀，黑客呀，我们与其斗争了这么多年，出现了这么多的产品，发现越到后面我们越被动，越是到现在越是不知所措，安全形势越来越严峻，以前的做木马做病毒的人是为了炫耀自己，现在做木马做病毒的人是一个产业链，盗取别人的东西进行交易买卖，形成了黑色的产业链，这个就比较可怕，互联网的风险越来越大，在你浏览网站的时候病毒悄悄的就感染了你的系统，时时刻刻盯着你的电脑资料，所以安全的风险越来越严峻。 业务持续的风险除了前面讲的这些风险以外，比如发生大的水灾呀，我们的IT会不会中断呀，比如2003年非典的时候，什么设备都没坏，但我的业务确断掉了，楼被封了，进不去，这也是IT风险控制要考虑的内容。 还有一个内容比较重要就是绩效风险，讲IT只是讲投入不讲产出，我们在IT上投入很多很多，不知道大家有没有这样一个概念，投入多少钱，实际上我这有几个统计数字，2005年我国在信息化建设上投入了2829亿，06年是3227亿，估计到2007年就达到4236亿，增幅是很快的，这里面的大头是谁呢，不说都明白，是电信，政府，银行，企

业投入也很大的，在企业里一定涉及到投入回报，投入产出比，但是我们IT上很少有人会去算投入产出，提高管理水平管理效益，提高多少呀不知道说不清楚，这里面也是有一个黑洞，要有一套方法把我们绩效表达出来，这样你才知道我们明年投入在什么地方，哪一点是浪费的，关于这个事情我们的嘉宾姚乐先生会在后面有一个演讲。 现在的法律法归要求的越来越高，比如刚才提到的SOX法，他是美国的一个法律，跟我们有什么影响呀，我们国内有很多上市公司，所以你也必须做依从性，为什么要依从性呢，什么法太严密了，以前我们说违法就违法了，会通告一个会批评一下，做出相应的处罚，比如现在很多的上市公司的老总补罚了10万20万，他也不在乎那点钱，这个法可不一样，首先罚的非常大，个人可以罚款到五百万美元，企业罚款到两千万，但这还不是最重要的，还有一件最重要的是要做牢，如果这个公司造假，CEO、CFO最多要做20年的牢，这个他就害怕了，这个法律对我们有影响，对全世界都有影响，我们国家现在财政部及相关部门组织这么一个专家组，正在研究中国的SOX法，可能未来两三年之内中国也会推行这套东西，要求所有的上市公司也要做控制。 做内控和我们做IT有什么关系呢？太有关系，我们这些内控怎么去体现，我讲财务报告不能造假，财务报告是在财务系统里，你那个财务系统不可能授权不完备，让人随便改，得保证它的可靠性，财务系统从业务系统那里来的，业务系统装在数据库里，数据库装在服务器上，服务器在网络上，完全串在一起，IT本身要可靠，要从IT一直到你的财务系统，都要可靠，有一个地方有露洞的话你都谈不上，所以说要SOX法实施起来这么难了，而且SOX法

离不开CIO，虽然SOX法只追究CFO、CEO的责任，如果CFO、CEO的日子不好过了，你CIO还跑得了嘛？所以最后统计SOX法有40%的工作量是在IT上。 讲了这么多的风险怎么办，实际上我觉得今天提出来就是要建立一套制度，或人治，靠某某人领导重视，还有我们要搞的典型政府信息化的典型，企业的模式，这东西只是昙花一现，企业要把IT做好一定把他变成种制度，决定IT能够真正做的好不是一两个人的技术，技术已经不是很重要了，技术的东西总是能买到，但是把技术控制好、用好靠的是制度，靠的是管理，最终靠的是人，所以我们要建立一个有效的制度安排。 回过头来我们发现国内的一些信息化建设走了很多弯路，我们有一点和国外有区别的是我们不太重视游戏规则的制订，IT一定先要把规则建立起来，包括制度和控制，建起来以后我们发现IT风险小多了，所以我们要强调建立一种制度，IT风险控制其实上就是企业重要的组成部分。 