IT 治理与风险管理

人与风险的基本观点

治理与风险的关系及在 IT 方面的一些相关问题，在国内学者和产业界的朋友交流的过程中都比较关注，关于人和风险主要包含以下三个基本观点：

第一个观点：风险具有双重性质，既有主观性也有客观性。在地球上因为有人，大家关注、而且试图想去管理这种风险，而火星上没有人，所以没有人去关心它、管理它。所以，风险离开了人就不成立，这也是风险的主观性的一个表现。在风险的基本的讨论里面，风险是主观的还是客观的，一直存在着争论，现在越来越多的人都认为他是客观，但是现在讲客观的时候，也不能忽视它最基本的主观性。它实际上是表现出一个双重的性质。

第二个观点：管理风险一个很重要的前提害怕。我们从小就被教育要勇敢、不要害怕，但人生来就会害怕的，这是上天赋予我们风险管理的情结，一个人如果不懂得害怕，那他还能管理风险吗？包括我们金融机构在内，公司治理一个基本点就是要让他的法人具有害怕风险的机制。

第三个观点：划分人类文明的标志是对风险的管理能力。这是现在西方非常流行的一本风险管理的书里的观点，作者是美国非常著名的老一代的投资家、金融家。他的这本书讲述了人类的文明史，其实也是讲风险管理的发展的历史，这个历史讲的一个核心的观点就是人类文明为什么会有差别、差别在什么地方，进步的文明和落后的文明差别在什么地方？归根到底一句话就是风险管理的差异。

治理的本质

治理的本质，这个概念非常流行，现在一般接触的都是世界经济与合作发展组织，OECD 的定义。它是一整套对公司进行管理和控制的体系，具体包括流程、习惯、政策和机构设置等。从本质上讲，是对公司利益相关方（Stakeholder）责权利关系的一种安排。它的最终目的是帮助企业实现价值目标，这

个目的跟公司财务的目的是一样的。

治理与风险

在治理的本质里面，我们要了解一个关键词就是关系的安排是对于利益相关者的，在这个利益相关者的安排里面，最核心的问题是什么呢？应该是风险。最近有一个刚流行起来的词叫“风险治理”，因为这个治理是要对整个机构进行管理控制一个基本的架构，这个架构里面实际上解决的问题就是人的责权利的关系问题，因为任何的商业机构，甚至包括非商业机构最重要的问题就是需要承担风险，包括我们的 IT 业务、IT 的管理行为也是承担风险，他们虽然不能直接地换取收益，但是有助于去换取收益，支持换取收益，或者从核算来讲也可以把它核算成换取收益。

这就说明治理最核心的问题还是要治理风险，公司治理风险要搞清楚一个最关键问题是风险的所有者。2002 年，我第一次到美国做访问教授，我有幸结识了我们华人在美国金融圈级别最高的，美国道富银行的首席风险官。道富银行在美国金融机构里面，总资产规模当时应该排在第五位，相当于我们国家的国有银行。他是这个集团银行的最高层管理者、首席风险官兼副行长。他跟我讲到，在接到 9·11 的飞机撞大楼消息的时候，他马上找到了董事会主席和 CEO，跟他们说现在要进一步明确谁是风险的所有者。因为接下来会发生很多事情，很多高管都聚在天上，现在落在哪个国家都不知道，这些风险最重要的要明确，谁来管理、谁来做？首先要讲这是谁的风险，这是所有风险管理的前提。

风险是所有者的，但是风险管理不一定由所有者直接管理。很多情况下，管理层要代理风险的所有者去管理风险，这些过程中自然而然就存在着委托代理关系、信息不对称的问题。我的第一本风险管理专著，在结尾的时候写过一段故事，就是说我做父亲之后，在带孩子与风险管理的关系中，我感触最深的一个问题就是风险治理的问题，因为孩子是我的，孩子是保姆带，我可以找一个很能干技术上过了关的保姆，但是当我看到很多网上披露保姆虐待孩子的事情之后，我就很不放心了，我恨不得在家里装上

摄像头，我又把我干妈请过来看着保姆。这就是委托代理关系，但是这个里面，孩子所面临的风险，是我这个做父亲的，我是风险的所有者，孩子长大了以后当然是回报我，他不会回报保姆。孩子受伤以后我最心疼，不是我的保姆心疼，但是管理风险是体现在管理保姆上。这个过程中，你去监督也好、激励也好，首先作为父亲，你要承担起责任来，这个问题的提出是风险治理的一个重要的内涵。风险治理是围绕着公司范围内的风险的承担和风险管理的决策权、问责与激励的一系列制度的安排，这才是风险治理乃至公司治理的主要内容和本质内容。

IT 治理的内容与目标

根据国际信息系统审计与控制协会(ISACA)的定义: IT 治理是一个由各种关系和活动过程组成的治理结构，用以指导和控制企业的 IT 活动，其目的是为了在平衡 IT 和 IT 活动所产生的风险与回报的过程中，通过增加商业价值来实现企业的目标。

从这些定义中我们看到，IT 治理的主要的内容、目标，是有利于管理好 IT 风险。IT 治理的利益相关方，它涉及到 stakeholder 概念的提出，就是让我们讨论问题有了一个更全面的视觉，当你论到 IT 治理的时候，跟 IT 利益相关的有公司或者银行的所有股东、董事会、大小股东，还有管理层面，IT 的使用部门、科技部门、风险管理部门、审计部门在 IT 相关事务中有不同的利益关系，事前、事后都有不同的一些制度安排，这些安排对于 IT 风险管理至关重要。银行的业务的使用者，还有我们的 IT 的供应公司、IT 的供应部门、监管部门，都是 IT 治理的重要相关方。当然随着我们对 IT 治理和 IT 风险管理更多的研究，可能更多的相关方会感受得到。你考虑得越全面，IT 治理的相关的利益方面考虑得更多的话，整个 IT 的风险管理向全面风险管理就迈进一步了。

IT 风险的认识

对 IT 风险的认识，首先一个是 IT 相关的风险。我想 IT 的风险不应该仅仅是 IT 本身出问题的风险，

比如说宕机、黑客等，其实有很多角度，当然首先是业务受到了影响的风险，我们的业务跟 IT 风险是紧密相连的。再一个就是声誉风险，IT 出问题影响到客户对你的看法，监管对你的看法，这是一个影响大家对你看法的事情。而我们知道，金融风险对于金融机构来讲甚至比资本还要重要，IT 风险跟所有的操作风险一样，不仅要损失钱，更重要的还是损失声誉、损失大家对你的信任。所以，IT 风险管理不仅仅需要考虑到当前的技术问题，还要考虑到技术发展的问题，还要考虑到法律环境的变化问题、考虑到市场竞争的问题，这些战略在未来三五年、甚至十年、二十年，这种业务的发展，不仅仅是 IT 技术的发展，什么云计算等等，现在很多的概念，还有业务本身对 IT 的要求，像风险管理里面对于 IT 的要求是很高的，这些 IT 系统在战略上能否支持整个公司的战略风险问题，也是应该考虑的。

另外就是数据与模型。像金融危机爆发以后，大家对于模型、数据方面的批评。前几天我接待一个华人专家，是前世界银行前首席科技官，也当过香港证监会的首席信息官，他现在想推进中国的数据与管理。他认为这种科技风险，其实应该也包括对数据、对模型的风险。通过模型与业务结合得更加紧密。所以，跟 IT 相关的风险是非常多的，不仅仅是 IT 技术的本身，跟业务、跟战略、跟模型都有关联的。

IT 风险的性质

对于 IT 风险的性质，首先 IT 风险仍然是操作风险为主，这个不会有太大的争议。为什么把它单拿出来，主要是 IT 风险特别重要，另外有它技术方面的特征。但不管怎么看仍然是操作风险，他具有操作风险的一般性的特征，我曾经总结过操作风险的几个基本特征：

第一是复杂性，操作风险其实要比其他的风险还要复杂，因为它引发风险的因素非常非常多，往往是市场风险、信用风险，往往是市场、利率、汇率的波动，信用就是客户的经营能力。而操作风险是方方面面的、众多的因素、数不清楚的因素来导致这个问题，包括 IT 的风险，所以它更为复杂。

第二还有普遍性，它是到处存在的。我想 IT 广泛的应用，也是一种典型的、具有普遍应用的风险。

IT 风险会带来收益了吗？这也是风险管理的基本问题，就是操作风险会不会带来收益？操作风险是

不是也符合以风险换收益的规律？从总体上讲，只要有 IT 业务，不管管理到什么程度永远会存在 IT 风险，总是会发生不同程度的 IT 风险事件。IT 风险和其他的风险一样，都是总体上不可避免的，但是它可以有大有小，你管理得严它发生的事情少一点，管理得松它发生的事情就多一点、大一点。当然要像一级 IT 风险是没有可能的，这是我们对所有风险的一个基本的判断，只要你承认这个观点，承担风险就是有必要有办法的，这个办法就是有必要的，既然是没有办法又是有必要的，它就是应该有价值的。你要干这件事情必须使用 IT、必须具有 IT 风险，那你干这件事情以后所获得的收益，必须在会计核算里面，核算一部分给 IT 部门，是我 IT 部门给你带来的，否则你这个事做不了。所以从这个角度来讲，合理地承担 IT 风险也具有以风险换收益的特征。

IT 风险管理的基本策略

第一种方法是规避。所有的风险管理里面实际上都一样，规避相当于《孙子兵法》的三十六计走为上一样，我惹不起还躲不起嘛。所以如果这个业务需要很大的 IT 的投入，或者 IT 风险我根本没法控制，我就不开展这个业务。但是你能够规避所有的风险吗？所以，规避只能是一个策略性的，只能对于具体的一项业务或者某种 IT 的应用来实现，而不能规避所有的 IT 风险。在这个里面，关于什么 IT 风险可以不承担？不仅是技术上的问题，现在从经济资本的角度也开始支持做这种决策。

第二种方法是如果你不规避，那么选择内部控制，这个事情正是目前我们大家每天都在做的工作之一。

第三种方式是对冲，这是风险管理一般的概念，对冲就是转移。转移最常见的比如说保险，比如说 IT 风险的操作风险，保险公司应该给设计产品，但这样取决于一个国家的保险公司是否发达，有没有足够的产品来满足金融机构对 IT 的需求。除了保险以外，外包实际上也起到了对冲风险的作用，如果这个 IT 不行的话，找一个供应商帮我做了，实际上也是一种对冲风险的行为。还有灾备也是典型的对冲风险的行为。

最后一种方法是定价补偿。不管怎么管理、如何承担 IT 风险，这种 IT 风险必须能消耗经济资本，因为我这个银行做下来必须要承担 IT 风险，最后贷款利率里面必须有一部分是反映 IT 风险的合理回报的。

IT 治理的模式定位、组织架构、职责分配、报告项目、风险文化建设、内部控制、风险管理、薪酬机制、审计活动等等，都是跟治理密切相关的。治理这个概念可以做得很大，可以包罗万象。比如说内部风险管理、操作风险管理跟内部控制的关系，大家也很容易混淆，还有合规管理等等。作为治理的，实际上是整体可以把这些风险管理都包含在内，为这些风险管理建立了一个基本的框架和基石。