风险评估和应对

一、风险评估概述：risk assessment可定义risk parameter并管理uncertainty，最终用于实现其财务目标。risk assessment过程包括risk identification和risk analysis

1. risk assessment定义：每个企业的运营过程都面临风险（结果的不确定性，可以是positive也可以是negative）。风险评估流程可为各层级管理层提供风险picture，全面的风险评估可让企业有效管理所有风险并知晓对企业的冲击。通过risk management(决定并实施企业最优风险水平的过程)，企业会重视风险评估，合适的风管可加强governance，compliance并可更好的识别机会和威胁。风险可分为pure risk（包括hazard risk（由property/ liability/ personnel loss引起）, operational risk（由人/流程/系统/control引起））和speculative risk（包括financial risk（由市场对资产和负债的冲击引起）和strategy risk（由经济和社会trend引起））。企业的size和operation决定了其面临的风险类型。

2. 风险评估的目标：告知管理层企业所有面临的风险，这些风险对企业目标实现的影响，以及潜在的风险应对方案。风险评估帮助企业形成完整的risk picture。不仅要考虑现有业务的风险，也要考虑可能出现的机会和威胁，同时要判定不确定性的后果（包括likelihood和consequence两方面）。

3. 风险评估流程：

（1）风管人员必须知晓公司risk appetite（公司在risk-return基础上愿意承担的一种或多种结果）和risk tolerance（愿意接受的uncertainty amount）及自身职责。

（2）风管人员同样需要了解风险评估和处置所用的tools和技术（如questionnaire，checklist，cause-and-effect分析，failure分析。通常基于公司需求，分为qualitative（更主观，如survey） or quantitative（基于数字和计算，更客观））。最有效的方式为qualitative和quantitative同时使用。

（3）风险评估方式分为top down或bottom up。top down会有公司高层或board of director参与，聚焦影响公司实现目标的战略问题。bottom up通常关注具体business层面问题，且更偏向于具体运营。两种方法需结合使用从而给出更全面的风险评估。

（4）risk identification（风险识别）和risk analysis（风险分析）是ERM的一部分。

-risk identification检查可影响企业实现目标或无法实现目标的内外部环境及相关问题，这部分需要了解所有possible risk，避免未知风险导致的结果。此部分需要知晓risk sources and risk exposure以评估潜在结果，对于identified risk，需要了解用于mitigation的possible control。

-risk analysis需要调查identified risk以决定是否需要risk treatment以及相应的技术。风险分析考虑risk的原因和来源及其正向或负向结果。可使用risk map（risk matrix，描述风险可能性和潜在结果）来评估风险分析结果，必须评估同一件事带来的所有结果，同时要考虑多重风险之间的叠加或抵消效应。风险分析时，还要考虑风险发生的可能性。

二、risk identification和risk analysis技术分类：具体使用何种方式取决于风险本质，数据可用性和其他因素。

1. questionnaire和checklist：最简单的risk identification技术，通常用于risk identification的开始和总结阶段（通常使用了其他复杂技术，总结时使用此技术），该方法弊端在于可能无法识别所有风险（有些问题被忽视）且无法产出quantitative结果。

2. workshop：在识别风险可能性及其影响方面较有效，风管人员可组织多部门/多职能/多stakeholder间的讨论，可从更宏观视角看风险且知晓不同部门间对同一问题的理解，进而对风险了解更全面。此方法弊端在于高层的观点会占更大的分量，应避免个人观点屈服于管理层意见。brainstorming优势在于引导更有创意的想法。Delphi属于头脑风暴，可基于匿名expert panel达到对某一问题的一致，其优势在于更多观点（匿名性保证）以及更广泛的专家意见（彼此不需见面），缺点在于time-consuming，此种方法通常用于复杂度中等，需要产生qualitative data的问题。

3. cause-and-effect analysis：此方法分析起因的可能性，用于对引起某一结果的所有问题的调查。该方法通常用于找出root cause及inter-relation关系。

（1）fishbone diagram（鱼骨图法）从最终问题和结果出发，向前推各种原因，继而组成骨架，之后最终找到isolated root cause。

（2）5 ways approach（五步分析法）从最终的问题和结果出发，持续提问why，从而向前倒推原因。通常此方法和鱼骨图同时使用。该方法通常适用于简单问题，弊端在于参与者有可能在找到最终的root cause前就停止，从而导致无法揭露真正的root cause。

4. failure analysis：聚焦失败原因的分析从而预防再次发生，如未完成业绩指标，机器损坏或房屋或存货损失。

（1）hazard and operability study(危害与可操作性分析，Hazop):解决复杂问题的，耗时较长的方法。聚集各方面专家研究具体流程并检视failure如何导致hazard（可使用guide word进行），最终团队会提交一份结论文档（包括treatment plan）。该方法通常用于制造业和流程运营方面（即潜在危险可导致直接的物理损失，员工受伤等）

（2）fault tree analysis（FTA，故障树分析法）：特定事件作为顶端，逐层向下分析风险和应对措施（层层向下，体现逻辑性），具体应对方式通常可减少事件的发生率和损失程度。此方法可系统检查所有风险。

（3）failure mode and effect analysis（FMEA）：检查系统或流程内每一步可能出现的问题，以及如何影响整个系统，也会分析可能性和损失程度。FMEA用于design阶段，且可评估人员问题。评估有问题后，及时修正设计。FEMA输出定性结果，用于中等复杂度的问题，可根据严重程度（criticality）对问题进行分类并排序，即failure mode-effects-criticality analysis.

5. future states analysis：决定未来会出现什么风险，通常使用scenario分析新事物（如新技术、新竞争者）如何影响现有环境。风管人员提出多种scenario及可能的结果。Monte-Carlo simulation使用随机变量从宏观角度评估风险，用于统计分析计算结果及各自的可能性。

6. strategy analysis：risk assessment可融入在strategic planning过程中，用于identify, analyze and evaluate潜在风险，此类计划可持续3-5年。风险评估需要和公司的战略目标一致，并识别影响目标实现的风险，此处识别出的风险可用其他risk identification和分析方法解决。

（1）常用技术为SWOT，先从企业内部的strengths和weakness开始，之后评估外部环境的opportunity和threat（通常会考虑宏观因素）。strength和opportunity合并为竞争优势，weakness和threat合并为risk to be avoid.

（2）PEST分析（political, economic, social and technology）用于分析企业的外部宏观环境，通常在SWOT内部分析opportunity and threat。

7. emerging tech and smart products：新技术可为其他方法（如SWOT）提供更多的数据支持，也可提供更多的trend和scenario（如future state analysis）。新技术(如侦测周围环境的sensor传感器，RFID tag（radio frequency ID）)可以提供real-time/ dynamic risk identification and assessment，之后可使用artificial intelligence（AI，模拟人类只能）和computer vision（模拟人类视觉）进行分析，进而预测风险。该技术不能替代其他risk identification和分析方法，但可克服一定的弊端，如可基于大数据准确快速发现更多outcome。新技术可帮助企业探寻risk scenario，更快的对风险作出identify和assess。

三、Risk Treatment：风险处置取决于risk assessment的结果。处理风险的常规技术包括avoid risk, 改变风险的发生率和损失程度，转移风险，自留风险，exploit risk。

1. Risk Treatment流程：treatment基于risk identification and analysis。

（1）有多种处理风险的手段，企业需要评估最后的结果。风险处置目标是改变已识别的风险，协助企业实现目标。风险处置的流程是连续的，需要检视某种或某几种处理方式实施后的residual risk（剩余风险，采取降低发生率或损失程度后等措施后，依然存在的风险），同时还包括选择并执行风险处置方案及对应的有效性。

（2）风险处置技术并非相互孤立，可以同时采取多种技术。risk treatment plan（风险处置计划）先确定风险优先度，之后选择对应的技术。审核风险处置计划在rm过程中非常重要，风险会随着企业运营和环境而改变（过时的风险处置方法有可能不再有效），新技术导致的风险也要进行相应评估。同时要考虑风险处置的成本-收益情况。

（3）risk treatment plan应将处置流程，treatment option，责任人，处置时间，monitoring及review时间都记录在案。

2. Risk Treatment技术：risk treatment技术适用于hazard/ operational/ financial/ strategy risk. risk treatment技术大致分为avoidance，modification，transfer，retention and exploitation。

（1）企业需考虑风险处置技术对speculative risk（chance of loss/ no loss/ gain）的影响；对于pure risk（chance of loss/ no loss, no gain），风险处置技术只需考虑管理好负面结果。

（2）对于有明显正向结果的时间，风险处置技术主要关注如何将正面结果最大化（exploit risk），此时需要增加事件的发生率，但也要同时考虑潜在的负面影响。

（3）risk avoidance：有时是最佳选择，但需要考虑相应的机会成本。

（4）risk modification（改变风险的likelihood和/或潜在影响（正面或负面））：对于hazard risk，loss prevention用于降低特定损失的发生率，loss reduction关注降低财务损失程度。企业可利用某些事件更改运营风险的结果。

（5）risk transfer: 风险可通过协议方式进行转移/ share/ 或与其他组织进行joint venture。对非重要工作，outsourcing（外包）可将相关风险share给其他业务方。对于hazard risk，保险是主要的风险转移方式。contractual risk transfer (non-insurance，如hedging or contractual agreement) 可用于将财务风险损失转移给其他业务方。

（6）risk retention（风险自留，将风险后果（可好可坏）留在企业内部）：用于风险处置后的residual risk（剩余风险），风险自留通常与risk modification和transfer同时使用。无计划的自留unidentified risk有时会给企业造成巨大损失，所以retention应用于已识别且已分析过风险（企业知晓自留了多少风险）。有时企业也可考虑多自留风险以扩大收益。

四、传统的accident analysis技术：可协助风管人员找到风险可能的原因并选择最合适的risk control技术。通过分析已发生的accident，风管人员可选择合适的risk control技术以防止其再次发生或减少相应的损失。

1. accident causation：意外由多种原因引起，通常有一个direct cause（一般是unplanned release of energy which cannot be absorbed by person or object.），大部分意外会有basic cause/ indirect cause (包括unsafe act和unsafe condition（如poor management/ safety policy/ personal or environment）)，风管人员需要了解导致意外的所有方面。

2. accident analysis技术：用于了解direct/ indirect/ basic cause of accident. 这些技术可从多方面分析accident，但没有一种技术可适用于所有情况。

（1）sequence of events (Heinrich的Domino theory，假设accident是一连串事件的最终后果): 该理论认为事件链由如下组成：ancestry/社会环境，人员错误（impulsiveness，violent temper, nervous等），unsafe act/ mechanical/ physical hazard（具体操作），意外本身，导致的损失结果。每个意外都由负面的社会环境开始，至造成损失结束。若去除前四项中任意一项，意外就不会发生；去除unsafe act/ mechanical/ physical hazard是最好的避免意外结果的方式（unsafe human act的重要性远大于unsafe condition，所以纠正unsafe act最有效）。该方法最适用于因human control/ human carelessness的situation，不太适用于处理自然灾害方面的accident。

（2）energy transfer theory（Haddon的理论）：energy release的amount或rate让物体无法承受，进而导致accident，即energy out of control。该理论关注控制energy release以及降低energy release导致的损失

（3）technique of operations review（TOR）：management shortcoming导致accident，该理论主要关注工伤和疾病，但也适用于财产/人员/责任/净收入损失等方面。该理论强调risk control的重点为unsafe act/ unsafe condition/ accident都是管理系统问题的征兆；特定情况会导致严重的伤害；safety应和其他企业部门一样进行管理（计划，组织，引导，控制）；管理层应当确定安全流程；function of safety用于确定并定义导致意外发生的operational error。后续理论认为管理问题主要体现于coaching不足，failure to take responsibility, 授权不清，监管不足。TOR体系中，管理层必须承认自身的错误并进行纠正，之后即可消除大部分accident。

（4）change analysis：预测某种改变对现有事物的影响。该方法可同时评估多种变化同时发生对结果的影响。

（5）job safety analysis（JSA，详细分析每项具体任务，找出潜在风险，并设定处置方式）：最万能的方法，最适用于重复性高的人员活动（行为和风险均可预测）。

五、system safety analysis：此方法由US Department of Defense开发，最初用于minuteman导弹研发和部署，后用于所有航空航天工业和实话和电力企业。企业可被认为是一个系统，企业内部也是各种系统组成，风管人员需要让这些系统安全有效运转。

1. 系统安全的定义（在整个系统生命周期中，考虑系统间关联的相互作用）：把组织看成整体，预测内部问题如何发生以及使用何种合适方式预防或减少损失，也为已发生的accident提供调查框架。系统安全依赖identify和分析hazard的各种技术，也依赖确定这些hazard如何导致系统failure/ accident的技术。这些技术可预估特定损失的可能性，并提出成本可控且有效的预防方式。该方法和其他关注unsafe act or condition的传统方法不同（传统方法中，一旦unsafe事件确定，就会提出相应的控制）。

2. 系统的概念：所有系统均有四个特点

（1）component：风管人员必须了解系统的组成部分。component属于system physical element，由于其可危害整个系统的可用性，所以需要特别关注，此项通常由传统风管或safety部门负责。其他形式的impairment（包括deterioration或technical obsolescence）通常由其他部门负责。但system approach消除了其中的分界，风管人员需要考虑all system physical elements impairment。所有系统均有sub-system（不管这种sub-system与system的层级差距有多深），某个sub-system出问题都会导致system的损伤。风管人员需要知道system及其所有subsystem，了解其相互关联关系，以及某个subsystem的失效如何影响其他subsystem或整体system。system一般由energy source驱动，所以energy也会成为一种潜在的风险。风管人员需确保energy的合理控制和system physical movement来保证system的完整性，同时确保energy持续可用以及整体系统按计划执行。

（2）purpose：每个系统都会至少有一个目标且需要支持system目标，风管人员必须知晓这些。

（3）environment：所有system均运行在一个大的environment中，对于大环境来说，system其实都是subsystem。

-直接的physical environment包括温度，illumination，pressure，working surface等。在极端条件下，系统可能无法正产完成其工作。

-organizational environment：系统运行须遵守的policy和流程。这些决定了组织内的授权和责任是否清晰，管理层对安全的责任以及员工提问的empowerment。

-socio-economic/ legal environment包括社会标准（norm）和convention（习俗），安全/环境和各种法规，以及local/ national/ global经济考量。

（4）life cycle：系统会经历五个阶段。

-conceptual phase（明确系统基本目的和初步设计）：构思阶段对hazard考虑的越多，后期运营时对其他保护设备的依赖及对人员错误的考虑越少。

-engineering phase（设定系统design，测试prototype）：使用同样规格创建prototype（原型），测试系统所有功能。

-production phase（developmental phase，生产实际system）：采用和prototype同样的规格生产。

-operational phase（deployment phase，系统实施阶段）：系统实际使用阶段，此阶段不太会增加新的安全措施（与之前步骤相比，此时系统已定型，很难改变）。

-disposal phase（termination phase，系统使用寿命到期，需要处理）：此时需要多考虑环境因素。

（5）系统安全案例：某个时间可以从小到大分成多个角度考虑，每个角度都有相应的风险处置方式

（6）system safety的优势：可按顺序提出loss control方式以增强相关系统的稳定性；由于系统规模逐层上升，可从内到外进行系统安全分析；可从发生率和损失严重程度方面减少特定原因导致的损失。

六、Hazard risk的risk control技术：hazard risk是由财产/ 责任/人员损失等导致的pure risk。

1. avoidance：停止不或从事有风险的活动，从而让future loss的possibility完全消除（降低发生率），这样也不需要未来额外的loss control或risk financing，但avoidance无法消除过去的风险（如产品责任风险），且有时avoidance会导致其他风险产生出来（用另一种风险替代了avoided风险）。使用avoidance时还要考虑完全避免风险导致的其他成本增加。有些风险是天然产生的，无法回避，所以avoidance的实际用途很受限。

2. loss prevention：降低特定损失frequency，但不影响severity（loss reduction关注此项），实际使用中，经常是loss prevention和loss reduction同时使用。loss prevention通常在事故发生前使用（破坏一连串导致accident的事件，消除或减小意外发生率）。在进行loss prevention之前应仔细研究accident是如何发生的。

3. loss reduction: 降低特定损失的严重程度。风管人员必须假设accident已经发生，并考虑事前或事后应做什么才能减少损失。loss reduction分为pre-loss measure(减少severity，同时减少loss frequency)和post-loss measure(只减少severity，通常关注emergency procedure，salvage operation, rehabilitation activity, legal defense等用于停止继续或减少损失的行为)。energy transfer理论大多推荐loss reduction方法。

4. separation/ duplication/ diversification

（1）separation（通过isolated loss exposure来减小single loss导致的损失）：将财产或活动分散到多个地点，可有效降低企业对某单一asset, activity, person的依赖。对于可只依赖某一处资产就能生产企业来说，separation是合适的，一处有问题，另一处的资产足够继续维持生产。

（2）duplication（复制，使用backup/ spare/ copy等将其储存）：备份的资产只有在主要资产损失后才会启用，可减少企业对单一资产的依赖。duplication和separation的区别在于企业依赖资产的频率，duplication的资产必须足够重要以抵消其备份的成本，如会计账本和记录。

（3）diversification（多样化，将风险分配给多个项目/产品/市场/地区）：旨在防止单一事件损毁企业的大部分资产，该方法主要处理business risk。

（4）separation和duplication的区别

-separation和duplication都不会降低损失的severity，企业仍有遭受损失的可能，但冲击会变小（因为有separation和duplication）。

-separation和duplication都旨在降低单个事件导致的损失，但在loss frequency方面不一致。separation会增加loss frequency，duplication增加的loss frequency会小很多。

-duplication会总体上减少average expected annual loss，因为其在小幅增加frequency的同时，可明显减少severity。

-separation可以减少average expected loss，不过这取决于在severity上的减少程度超过在frequency的增加程度。

-可更好预测loss exposure的增加和每种loss severity的减少，特别是exposure unit的数字足够大后，即可遵循大数法则。

（5）separation和duplication通常成本较高且不利于管理，separation通常属于其他管理决策的副产品（by-product）。高管通常知晓特定资产的重要性，所以duplication通常出于风管考虑来设置（如record，spare machinery parts, cross training employee）。通常来看，separation比duplication有更多实际用处。

-separation的好处包括：分多处储藏零件；运营时每辆卡车只需留出一些负载即可（如某些车发生问题，其他卡车满载即可解决问题）；如果某一地点出问题，其他地点可接替继续维持企业运营。

-duplication的好处包括：只有在原件损坏后才启用备用文件；保证有后备机器支持生产；可帮助同类型企业渡过难关。