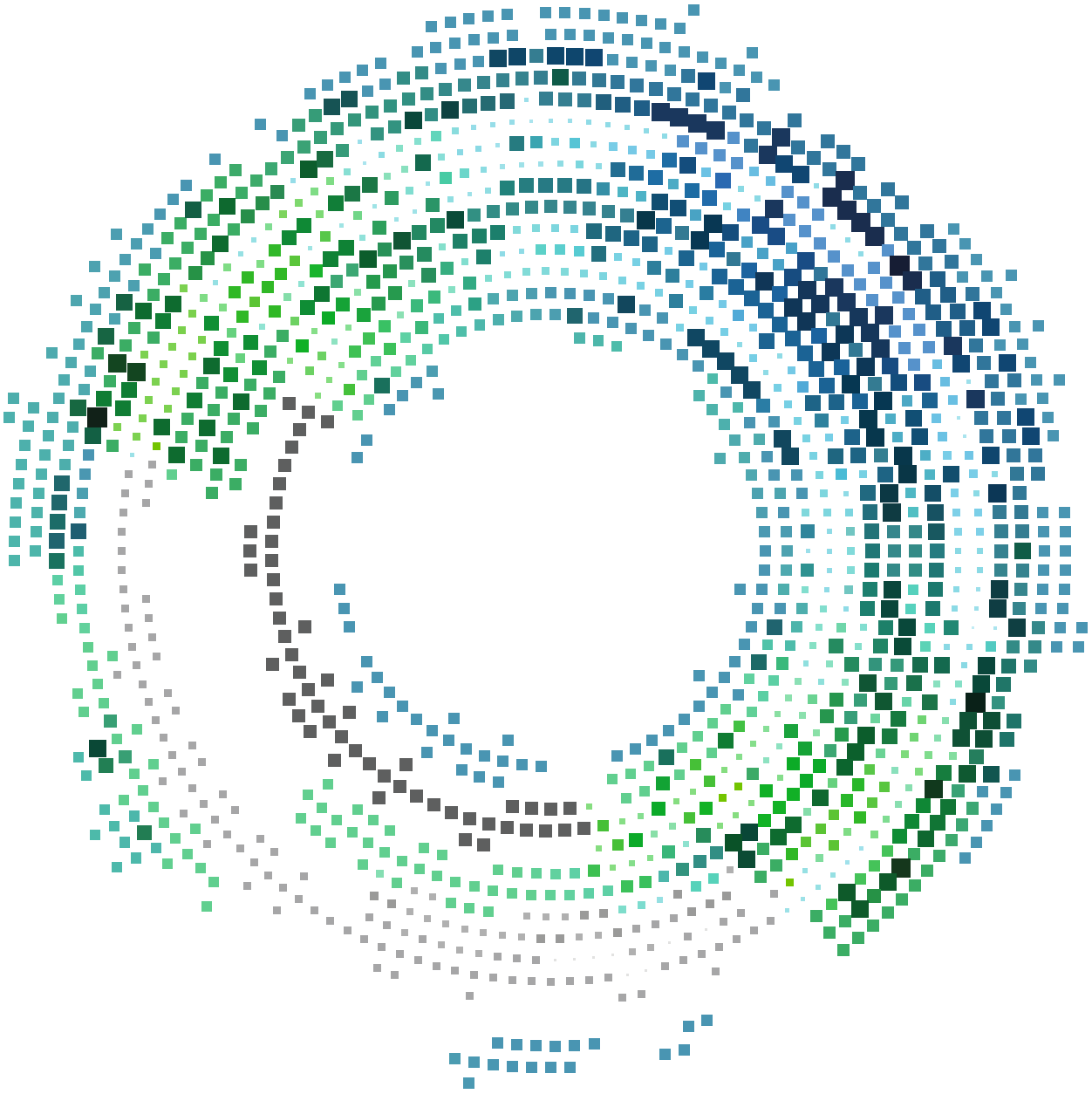
Deloitte.

德勤



网络风险

风险驱动绩效

Cyber

评估网络风险

董事会和高管层需要面对的关键问题

风险驱动绩效

一直以来，在人们不遗余力保护企业的业务价值时，风险被认为是需要最小化或应当规避的。然而，我们相信风险也能创造价值，而且，如果可以被正确处理，它将会在驱动业务绩效上发挥独特的作用。

以网络风险为例，随着信息技术的广泛应用和企业全球化进程的深入，企业面临的网络风险日益凸显，但另一方面，它们同样为企业提供了关键的竞争优势。那些因为过于重视保护企业业务价值而拒绝接受信息技术应用和全球化运营的企业，终将落后于这个时代。而那些擅于管理网络风险的企业则能从信息技术应用和全球化机遇中缔造卓越绩效。

踏上风险管理旅程的关键一步是了解贵企业自身网络安全能力现状。本文和文中包含的网络安全能力自我评估工具旨在帮助企业高管们衡量企业自身的网络安全成熟度，帮助其形成网络风险新认知，并解答一些关键问题，包括：

- 我们是否有合适的领导和管理人才？
- 我们是否关注且进行了正确的投资？
- 我们如何评价企业网络风险项目的有效性？

如今的行业领导者们已经学会了通过风险管理来保护业务价值，而未来的领导者将是那些抓住机遇，利用风险创造价值的佼佼者。德勤全球风险管理专家将引导您踏上这段旅程，并帮助您将贵企业打造为风险驱动绩效的典范。

风险管理责任

网络风险对于企业中的每一个人都至关重要，然而监管风险的最终责任则落在高管们头上。

现在，许多董事会成员和高管们很少接触日常的风险管理活动，包括网络风险的监控、检测和响应等。但那些对企业现状，特别是对网络风险现状有深刻了解的领导们，对于如何更好地管理企业有着自己的独到见解。

有效的网络风险管理始于董事会和高管层的重视。通过回答一些重要问题，提高认识风险、管理绩效的能力，进一步提升风险管理成熟度水平，企业的业务运营终将变得更加安全、警戒和具有韧性。有别于传统网络威胁管理仅聚焦于安全，而少关注警戒性（全面监控所有威胁）和复原能力（对攻击的反应能力和恢复能力）的情况，这三点对于现今的业务活动尤为重要。下列十个必须回答的深度问题，将有助于企业管理层更好地理解他们所处的境况以及什么时候他们的企业将变得安全、警戒和具有韧性。

1. 我们是否对网络风险开展全面评估、确认其归属并进行了有效管理？
2. 我们是否有合适的领导和管理人才？
3. 我们是否已经建立起反映我们风险偏好和预警阈值的，恰当的网络风险上报机制？
4. 我们是否关注且做了正确的投资？如果是，我们如何评价和衡量我们的决策结果？
5. 我们的网络风险管理工作和能力是如何满足行业标准和符合行业发展趋势的？
6. 我们是否在全体范围内形成了以网络风险为中心的思维方式和网络风险意识的企业文化？
7. 我们做了哪些工作来保护企业免于第三方网络风险？
8. 我们能否遏止由于网络安全事件导致的损失，并且调动相关资源进行应对？
9. 我们如何评价企业网络风险项目的有效性？
10. 我们是否是企业紧密关联的生态系统中强大且安全的一环？

董事会和高管层在帮助企业应对持续变化的网络威胁环境中扮演关键角色

当前，网络威胁和攻击越来越多，并且越来越复杂。与此同时，不同业务领域间的联系越来越紧密，数字化发展趋势也越来越明显。置身于这样的新环境，网络威胁管理获得了前所未有的重视，成为企业业务和战略层面势在必行的关键活动。当前，由于庞大犯罪网络，外国政府支持的黑客和网络恐怖分子的频繁活动，网络犯罪的定义不断拓展：网络犯罪并不仅限于诈骗和盗窃，已包含服务中断，数据破坏或损毁，以及从受害者处获得财物、访问权，或凭借窃取的企业机密进行敲诈勒索。

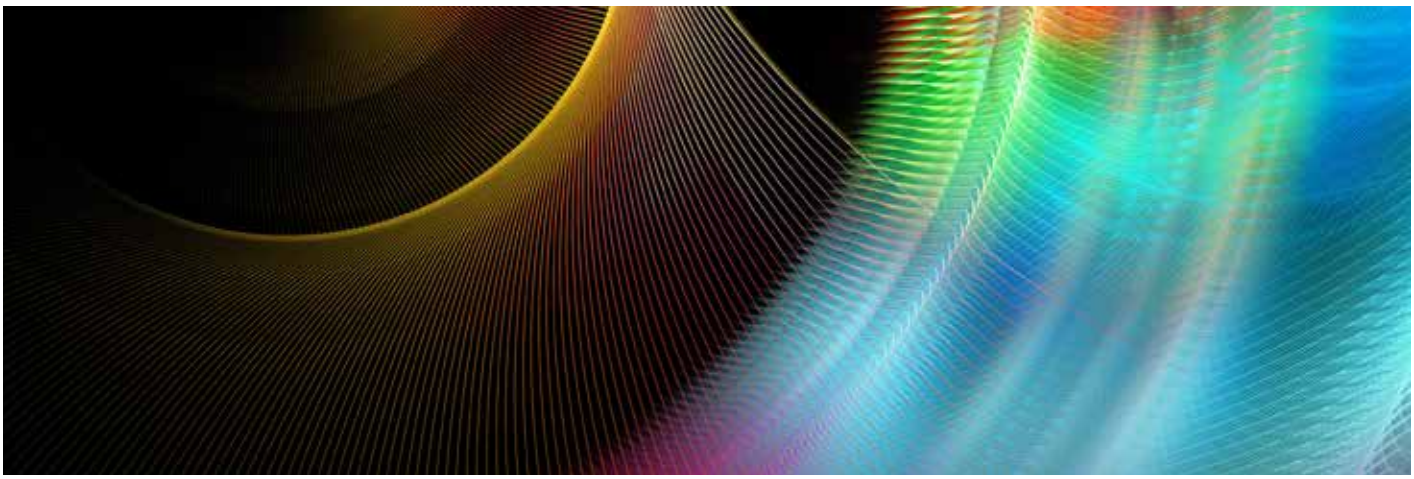
如今，网络风险和绩效更加紧密地交织在一起。网络犯罪导致的有形损失，包括被窃取的资金、受损的系统、监管罚款、法律赔偿以及对受影响当事人的经济补偿；无形损失则包括由信息化资产被窃导致的企业竞争优势消失、客户流失、业务伙伴失信以及企业声誉和品牌形象的全面破坏。除了对企业个体造成损失之外，网络攻击更为广泛的影响可能会导致基础设施大面积中断运营，进而影响到整个国家金融体系和经济的稳定。

重中之重

情势严峻，董事会和高管层也越发意识到网络风险必须作为首要的业务风险对待，并且要提高这种风险意识，使之根植于企业文化中。目前企业业务活动的各方面都涉及数字信息，因此网络风险意识不应仅限于信息技术部门和企业内部，而应扩展到每一个合作伙伴、每一位客户、每一名员工以及每一项业务流程。

企业高管应时刻保持企业终将被入侵的风险意识，对网络威胁开展研究了解，明确对企业影响最大的威胁是什么，而这些威胁又将会把企业重要资产置于何种危险之中？当高管们以这种积极态度去保护企业业务价值时，不少人会困惑如何才能保证他们的努力不白费？他们到底担负着什么样的责任？他们应重点培养哪些能力？哪些是应当解决的关键问题？面对这么多困惑和不断进化的威胁环境，如何备好万全之策异常艰巨。所以高管们应为或有事件，而不只是可能事件，做好预先准备工作是一个审慎向前的选择。

面对挑战虽然没有绝对的解决方案，但是董事会和高管层可以从开发定制网络安全计划或改进现有方案着手。而后文中，我们抛出的十个问题也将帮助推动董事会进一步讨论管理层面可持续的网络安全策略，包括如何面对不断变化的挑战，如何消除网络风险，以及如何抓住机遇？



评估贵企业的风险成熟度

该网络风险关键问题（及其影响范围）清单可有效地指导企业对其网络安全态势进行评估，促使信息安全团队专注于关键问题，以便提供关键信息，协助企业开展持续监测并不断提升其网络弹性。这些问题旨在帮助你确定具体的优劣势，以及改进方法。请贵企业在回答后文中问题时，自行判断符合贵企业网络安全成熟度的描述：

网络安全成熟度：

高
企业在网络风险控制方面拥有较高水平。

中
网络风险控制措施到位，但仍有部分待改进。

低
网络风险管理滞后，仅有有限控制措施，核心措施有待改进。

安全、警戒和恢复响应的企业意味着什么？

安全

建立并持续维护基础的安全性能——通过加强风险优化控制，来应对已知和潜在的威胁，同时遵守行业网络标准和法规。

警戒

在企业生态系统的各个领域，通过良好的态势感知发现违规和异常现象。

恢复响应

具备在遭受不可避免的网络攻击后，快速回到正常运营状态和弥补业务损失的能力。

1. 我们是否对网络风险开展全面评估、确认其归属并进行了有效管理?

在领导层面建立恰当的问责机制是必要的。如果所谓“监控”只是偶尔每五分钟更新一下网络安全事件状况，这很有可能并不能被称为有效的风险管理。

高成熟度

- ☐ 董事会和高管层对网络威胁的风险管理有决策权，并且负责监督网络风险计划的开，并确认其实施效果
- ☐ 董事会和高管层能及时了解网络威胁本身及其对企业的潜在影响
- ☐ 董事会中包含一到多名了解信息技术和网络风险的成员，或在该领域可信赖的战略顾问
- ☐ 企业的高管委员会，或由管理层和董事会共同组成的委员会，或兼职高管委员会，拥有充足的时间专门负责整体网络规划，专注于网络风险问题
- ☐ 网络风险全面评估在定期 更新、预算分析和向管理层质 询时是必须的

中成熟度

- ☐ 网络安全问题是领导层和董事会关注的重点，但对于具体架构的沟通和监管流于表面
- ☐ 董事会具备信息技术和网络风险的基本知识
- ☐ 缺乏网络安全尽职调查和就此向管理层质询的能力
- ☐ 董事会没有持续地关注网络安全框架和战略需求，并形成定期评估机制

低成熟度

- ☐ 企业顶层缺乏对网络安全的关注以及对安全领域战略性问题的了解
- ☐ 领导层在具体信息技术安全问题分析与解决方面参与度低
- ☐ 董事会在信息技术和网络风险方面缺乏经验，而且网络问题只停留在技术层面
- ☐ 网络风险的监控和相关要求的评估没有实施或成效有限

2. 我们是否有合适的领导和管理人才?

企业中的每一个人在网络安全风险方面都负有一定的责任。由于人人有责，也由于许多领导仅忙于履行传统职责，企业并没有做到任命一位合适的领导者，一位应当对网络风险管理直接负责的领导者。

高成熟度

- ☐ 网络安全领导具备将科技与业务结合的能力，能理解企业运作，发现业务机会，并知道工作优先级
- ☐ 网络安全管理团队充满激情与活力，始终紧跟最新的网络安全趋势，对最新的网络威胁及其对企业业务的影响保持关注
- ☐ 董事会和高管层关注并经常讨论网络风险
- ☐ 在相应领域有足够数量的具有相关行业经验的技术人员
- ☐ 对风险管理人才的薪酬和奖励机制与网络安全在该企业的重要性相匹配

中成熟度

- ☐ 任命的网络安全领导仅关注网络安全的技术层面
- ☐ 网络安全领导具备一定行业知识，但并不能完全理解企业运作
- ☐ 网络安全风险管理已成为重要的关注点，但只限于相对抽象的层面
- ☐ 网络安全风险问题通常停滞在信息技术或管理层
- ☐ 已有具备一定经验的人员在信息技术和部分业务领域任职，但他们对针对行业的具体威胁了解有限

低成熟度

- ☐ 领导层缺乏对网络安全风险的关注
- ☐ 信息技术职能中网络安全知识和能力是分离的
- ☐ 针对特定的新技术开展了专门的培训项目
- ☐ 因在战略层面缺乏对网络风险的人才投入，导致人员流失率高

3. 我们是否已经建立起反映我们风险偏好和预警阈值的，恰当的网络风险上报机制？

尽管当发生网络安全事件或疑似事件时，在更广泛的企业范围内发布网络事件信息，有助于加速信息的扩散和事件的处置。但是清晰地定义触发机制或阈值信息，以及事件报告路径，能够实现有效的网络风险事件响应和处置。

高成熟度

- ☐ 在现有的风险管理和治理过程中明确阐述了风险偏好和网络安全风险
- ☐ 企业整体的网络安全风险制度经由董事会审批通过
- ☐ 明确描述并执行了网络安全风险方案中的角色和权限
- ☐ 对于重大 / 关键网络事件，设定了关键风险点和绩效指标，规范了上报打破限制或阈值事件至高管层的流程
- ☐ 事件管理框架包含与网络安全风险处置方案一致的事件上报原则
- ☐ 已实施针对网络安全预防措施的评估与监测

中成熟度

- ☐ 现有的网络安全风险制度并未在信息技术部门之外完全落实
- ☐ 网络风险仅在整体风险管理和治理流程中被提及
- ☐ 风险偏好并没有被整合到网络安全风险框架中
- ☐ 对待网络安全风险的响应往往是被动，而非主动
- ☐ 兼职高管委员会有足够时间商议网络安全框架的实施

低成熟度

- ☐ 缺乏正式的网络安全框架
- ☐ 风险升级都是在事件发生时临时决定的

4. 我们是否关注且做了正确的投资？如果是，我们如何评价和衡量我们的决策结果？

在风险与绩效紧密关联的情况下，领导层应当了解企业将资源投向何处，领导层是否规划了合适的资源以应对网络安全挑战。没有开发并实施人才战略，服务方面的过高投入，以及其他运营成本的拖累都是实际存在的风险。

高成熟度

- ☐ 企业所有活动都将网络安全风险纳入考虑，从战略规划到日常运营，深入企业的每一方面
- ☐ 投资重点在安全控制基准，以应对大多数威胁，而战略性的专项资金主要用于企业核心业务和核心信息的风险管理
- ☐ 企业在识别“黑天鹅”风险方面做出了努力，并具备相应方案预防和避免这些虽不太可能发生却具有潜在灾难性风险的威胁
- ☐ 企业有清晰的投资业务计划，会根据风险调整企业投资和预算，并且体现在网络安全战略中
- ☐ 高管层为企业网络安全框架的实施提供了充足的资金和资源
- ☐ 已建立可靠的质询机制

中成熟度

- ☐ 网络安全框架着眼于企业内部，并不考虑行业特性
- ☐ 网络安全战略与企业投资并未保持一致，也不互相支持
- ☐ 企业的安全控制基准与防御复杂度较高的攻击之间的资源投入不平衡
- ☐ 在企业基础设施和应用系统保护方面具有强烈的威胁意识
- ☐ 已实现身份识别信息的保护
- ☐ 已实现自动化信息资产漏洞监测
- ☐ 缺乏“黑天鹅”风险的预警机制

低成熟度

- ☐ 缺乏网络安全战略，源动力和投资计划
- ☐ 只有基本的网络保护 / 传统的基于签名的安全控制措施，缺少对新技术和新方法的关注
- ☐ 偶尔进行信息资产漏洞评估
- ☐ 网络安全投资的计划较少

5. 我们的网络风险工作和能力是如何满足行业标准和符合行业发展趋势的?

通过与那些能够有效解决网络风险的企业进行比较，从而了解自身企业在哪些方面落后是很重要的。可是当你发现你已落后时，你将如何应对？如果董事会和高管层没有主动承担此项工作，那么谁来承担?

高成熟度

- ☐ 企业制定了全面的网络安全方案，根据行业标准和最佳实践来保护和侦测已知风险，保持对新型威胁的敏感度，并及时采取应对措施，开展恢复工作
- ☐ 采纳行业框架来建立、运作、维护和提高 / 改进网络安全方案
- ☐ 企业邀请外部机构对其网络安全方案进行基准评估
- ☐ 企业会定期确认其内部管控措施符合企业制度、行业标准和法律法规的要求
- ☐ 企业适用的关键领域业务已通过正式认证 (例如, ISO 27001:2013 证书)

中成熟度

- ☐ 企业的网络安全方案已实现了一些行业最佳实践，包括基本的线上监控、恶意软件自动化取证、手动电子搜索、罪犯 / 黑客监视、员工 / 用户行为分析、以及针对内部用户的跨平台监控
- ☐ 可能偶尔开展合规性或其他内审检查，未建立定期执行机制

低成熟度

- ☐ 网络安全措施都是临时的，且很少参考行业标准和最佳实践
- ☐ 为了迎合合规和监管要求，高管层可能会进行不定期检查

6. 我们是否在全体范围内形成了以网络风险为中心的思维方式和网络风险意识的企业文化?

由于企业努力加强其网络安全，使之更安全，警戒和具有韧性，许多业务聚焦于宣贯和意识培训。但随着这方面需求的深入，如何改变企业行为习惯？董事会和高管层应当给出指导意见。

高成熟度

- ☐ 从企业顶层给出明确指导，强力推动风险文化，以及可承受风险 / 回报思维
- ☐ 员工的个人利益、价值观和道德水平与企业的网络安全风险战略、风险偏好、风险容忍度和解决方法相一致
- ☐ 执行官们以开放和求是的态度就网络安全风险问题进行讨论，促进共识
- ☐ 企业层面围绕网络安全风险开展了广泛的教育和知识竞赛 (囊括全体员工、第三方、承包商等)
- ☐ 针对员工个人的意识培训帮助员工更好的理解其在网络安全风险方面的职责
- ☐ 员工承担其风险管理方面的个人职责，同时在需要时积极寻求他人的协助

中成熟度

- ☐ 有常规的信息安全意识培训
- ☐ 有针对资产风险管理和威胁类别方面的网络安全意识培训

低成熟度

- ☐ 有约定俗成的使用策略
- ☐ 很少强调信息技术以外的网络安全风险
- ☐ 意识培训开展比较被动，只有在违规行为被发现后少部分个人参加

7. 我们做了哪些工作来保护企业免于第三方网络风险？

企业许多违规行为的根源在于企业的合作伙伴，例如承包商和供应商。网络安全的关注点远远超出了企业自身业务范围，需要企业时刻与合作伙伴保持一致，了解他们的工作内容，以确保企业能没有压力地接受由合作伙伴带来的风险因素。

高成熟度

- ☐ 网络安全风险在关键外包 / 分包协议的尽职调查中是重要组成部分
- ☐ 所有与第三方相关的业务均经过统一流程，相关制度及控制措施到位，而且第三方能够满足企业的期望和风险容忍度
- ☐ 针对相关需求和风险，第三方需接受网络安全事件方面的培训
- ☐ 风险管理方案涵盖分析和评估所有重要的第三方关系和信息流
- ☐ 相关流程确保来自第三方的网络安全事件得到及时通报
- ☐ 基于对第三方的分析和风险评估，已采取措施来降低外包协议导致的潜在网络安全风险

中成熟度

- ☐ 已采取措施来降低外包协议导致的潜在网络安全风险
- ☐ 鼓励但不强制执行对外包和分包协议的尽职调查
- ☐ 如何与第三方就网络安全事件进行沟通并未列入合同条款
- ☐ 具备一定的分析内部威胁与外部威胁相关性的能力

低成熟度

- ☐ 只有基础的网络保护措施
- ☐ 缺乏对第三方的尽职调查和网络安全风险保护措施

8. 我们能否遏止由于网络安全事件导致的损失，并且调动相关资源进行应对？

即使在安全度很高的企业，往往也要花费几天甚至几周才能发现一个入侵活动。重要的是企业是否对自身安全威胁响应机制拥有信心。从领导层的角度考虑，关键的事件响应能力应包括明确且现成的指令链，通畅的沟通渠道（包括后备支持人员），以及对法律问题、公共关系需求、品牌形象和运营影响的全面审视。

高成熟度

- ☐ 有应对安全事件 / 安全事故的明确的汇报 / 决策上传下达渠道
- ☐ 网络安全事件响应制度和流程与现有业务连续性管理及灾难恢复计划有效结合
- ☐ 危机管理与网络安全事件响应计划和流程已发文实施，并经过实战、模拟、团队互动等形式的演练
- ☐ 已针对网络安全事件建立了与重要利益相关人的外部 / 内部沟通机制
- ☐ 企业积极参与行业模拟演练及培训

中成熟度

- ☐ 已建立基本的网络安全事件响应制度和流程，但是未能与业务连续性管理和灾难恢复计划形成有效结合
- ☐ 定期开展信息技术网络攻击模拟演练
- ☐ 业务层面不定期开展网络攻击演练

低成熟度

- ☐ 实施了一些信息技术层面的业务连续性和灾难恢复演练
- ☐ 网络安全事件制度、响应计划以及沟通渠道基本没有或完全不存在

9. 我们如何评价企业网络风险管理的有效性?

这个问题的答案很简单。将风险方案从头到尾评估一遍。但实际上，这个答案执行起来却有难度。此外，还存在一些挑战：企业需要学会跳出科技范畴，从业务角度来看待网络风险对业务活动和业务范围的影响；审查也不应限于信息技术，还需要包括业务流程。这些挑战都需要董事会和高管层的共同参与。

高成熟度

- ☐ 董事会和高管层确保网络安全方案的有效性得到评估和审查。已发现的薄弱环节已得到适当管理并且满足风险偏好
- ☐ 董事会，或者董事会的一个委员会，负责定期审查和讨论企业网络安全框架和实施策略，内容涵盖现有风险消除控制活动的充分性
- ☐ 定期针对漏洞开展内部和外部评估(健康检查，渗透测试等)，以便确定与行业内网络安全控制的差距
- ☐ 监督工作包括定期的网络安全预算评估、服务外包、事件报告、评估结果和制度审核 / 批准
- ☐ 内部审计将网络风险管理有效性的评估作为季度审查的组成部分
- ☐ 企业要求相关人员参加重要课程，以改进风险管理方案，应对不断变强风险，提高企业的安全性和警惕性

中成熟度

- ☐ 企业根据固定不变的时间表开展缺少行业特性的基本网络风险评估
- ☐ 内部审计每年对网络风险管理有效性评估不超过一次
- ☐ 不定期间歇性开展相关培训课程，以提高对网络风险的管理能力

低成熟度

- ☐ 极少甚至没有网络安全评估和内部审计评估
- ☐ 网络安全控制措施保持相对稳定，而且改进也缺乏经验基础

10. 我们是否是企业高度关联的生态系统中，强大和安全的一环？

合作伙伴的网络安全程度会影响到企业的网络安全态势，然而这种影响是相互的。你是否就是那薄弱的一环？你是否能主导网络安全风险管理？面对网络和更广阔的业务环境，你是否起到了积极的影响作用？与同行企业和合作伙伴合作，共享威胁情报，这只是领导层可以采取的紧密结合同业，更为全面地应对网络安全风险的一个范例。

高成熟度

- ☐ 与企业内部利益相关者、外部合作方、执法机构、监管机构保持稳定关系
- ☐ 支持创新的，不损害信息安全和隐私的分享
- ☐ 与同行、独立分析企业、政府、情报机构、学术机构和科研机构共享知识和信息
- ☐ 扩大共享范围到合作伙伴，客户和终端用户
- ☐ 优先选取能够支持行业标准，促进网络进步的供应商
- ☐ 独立维护成熟的项目，以避免成为最薄弱的环节

中成熟度

- ☐ 与同行分享威胁情报，积极与政府和私营机构在威胁方面进行合作

低成熟度

- ☐ 很少关注与外部机构的关系发展，缺乏与同行、政府或外部机构的知识和信息共享

设定更高目标，设定战略目标

不论你是想创建一个新企业或完善现在的企业，设定一个网络安全方面的成熟目标状态至关重要。而这个目标状态的有效定义是对业务内容和结果优化形成的一个全面认识，是与网络安全领导和企业其他决策者深入讨论的结果。并不是所有企业在网络风险的各领域都需要达到最高级别，定义网络安全方面的成熟目标状态也应该要考虑成本和时间的平衡，并应支持企业整体战略目标的实现。在很多情况下，这条路径驱动企业在关键的网络风险活动中朝着更高级别的成熟度努力。建立一个成熟的、先进的网络风险体系并不仅仅只是花钱花得不一样。它意味着采取一个完全不同的方式，通过投资于适用于企业的，安全，警戒和具有韧性三个目标的平衡组合，来建立满足于贵企业发展需求的网络安全体系。

贵企业的现状如何?

根据你的评估结果，贵企业目前的成熟状态是否支持甚至高于其整体战略和愿景？如果贵企业的成熟状态与目标状态不符，或者你还并没有建立恰当的网络目标，现在正是着手提高你们网络风险状态的最佳时机。

当然，对任何企业而言，百分百的安全是不可能的，但是有效管理并大大降低网络威胁带来的影响是完全可能的，不论这些威胁的影响是盗窃、监管罚款、法律赔偿还是声誉受损。通过一起努力，不管在本国还是全球范围内，我们都可以使不断增长的基础设施运行中断和业务中断风险最小化。

网络危机管理

就绪、响应和恢复

就绪、响应、及恢复

被黑客攻陷的设备，崩溃的网站，被破坏的网络，服务被拒绝，被复制的邮件，被盗用的信用卡数据，以及其它网络安全事故已经司空见惯。这足以使人们产生一种观念——是的——没有任何企业可以实现完全令人放心的网络安全。

大多数企业都因此培养了一定程度的网络安全事件响应 (CIR) 能力。但这些能力往往倾向于进行短期响应以及解决IT问题，可能无法消除网络安全事件带来的所有影响，或不让它上升到“危机”的程度。

避免网络危机需要在事件发生之前、之中和之后均能对其进行妥善处理。这是网络危机管理的普遍观点。管理人员经常将网络事件视为“IT问题”，而IT只是涉及其中的一个领域而已。

有远见的管理团队认识到有效的危机规划涉及多个部门，需要多种能力。他们还认识到当快要发生某个事件，或事件将要上升到危机程度时，他们必须高度协调合作来应对。

危机规划的必要性

CBS.com 指出，每年发生 150 万次攻击，这意味着每天超过 4000 次攻击，每小时 170 次，或每一分钟近 3 次攻击。[1] 虽然真正成功的攻击很少，但是事件的高概率决定了每一个企业都应当做好准备以进行有效应对。

整个危机管理生命周期都强调有效的准备（见图1）。

生命周期的每个阶段都是保护企业免受来自事件所产生的的风险、成本及损害的机会，并能强化企业的防御能力：

就绪

就绪并不仅仅等同于预警，例如7*24的实时监控，同样也是资源的就绪。一个精心准备的、多职能的团队必须准备好应对事件或危机的方方面面。此外，危机模拟和实战演练使管理层能够了解到什么可能发生、什么可以采取哪些步骤、以及企业是否真的做好了准备。

响应

管理层的响应可以是处理事件，也可以是升级事件；事实上，不当的响应甚至会制造新的危机。对事件积极而协调的响应可以有效控制时间、金钱、客户、以及声誉的损害和恢复的成本。管理层还须要准备好和各类媒体的沟通，包括社交媒体，让利益相关方知晓企业正在以恰当的方式应对当前的形势。

恢复

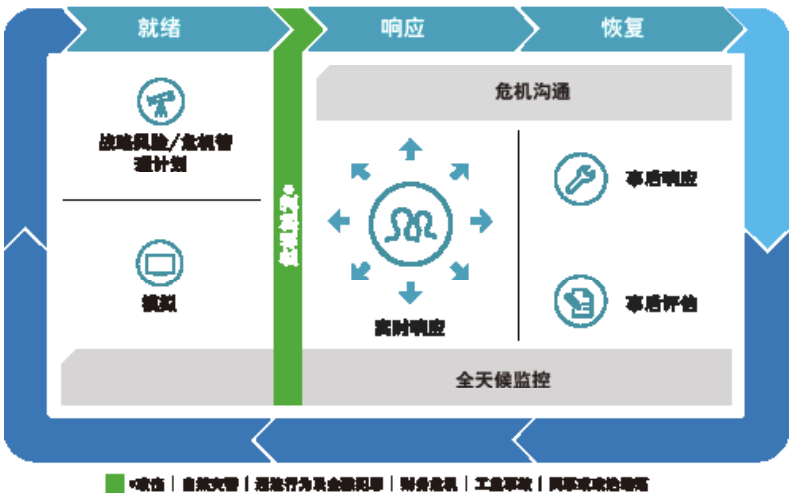
在事件或危机之后需要恢复到正常运营状态，并控制对企业及利益相关者的损害。事件后还需要进行原因的分析、对事件与危机管理的评估、以及经验教训的总结等活动。

有效的危机管理须从针对特定事件发展为一种更广、更灵活的能力，能从不同的维度对广泛的事件进行响应。从网络安全的视角来看，全局管理网络危机，可以促进企业更加安全，警戒和富有韧性。

IT及数字资产现今已是企业价值的主要组成部分。攻击者同样知道这一点，并理解系统的漏洞，他们会盯准企业，从不同角度反复尝试攻击。因此，危机造成的声誉、品牌、运营、客户和供应商关系风险会持续增加，也会产生相关的法律及财务影响。

再强的董事会或高管团队也不会有百分百的信心否认威胁的严重性，或者危机发生的几率 。因此，最好的方案就是在事件发生之前就准备好有效的危机管理计划。

图1 德勤危机管理生命周期



1 CBS 新闻，这些犯罪统计将使您再次思考：当您需要CSI团队时，他们在哪里呢？

安全，警戒和韧性

在追求安全的过程中，一个企业应该努力做到：

安全
一个安全的企业应认清其数字资产的价值，重点关注那些对企业最重要的资产。数据的重要性是不相同的，保证所有数据绝对安全是不切合实际的，并且也不可能满足的。通过对数字资产的价值进行优先级排序，管理层可以根据资产的价值来分配资源，从而提供与资产价值相对应的安全水平。

警戒
警戒要求每个人都能了解他们会如何通过自己的设备、社交媒体和网络行为使企业暴露于风险之下。警戒依赖于威胁情报的搜集以及对有可能损害企业的威胁范围的评判。这些信息也会作为威胁监控的输入。此外，针对事件的政策制定、培训和职责划分也对保持警戒起到关键作用。

韧性
一个具有韧性的企业目标在于最大限度地减少事件对其利益相关方面利的影响，同时能快速地恢复其业务、信誉和安全。事件的快速侦测及有序的恢复计划往往能控制损害。恢复计划应指定明确的角色、职责和措施来减轻损害，减少未来的风险，缓解现状，并恢复到正常运营状态。

一个安全，警戒，具有韧性的企业拥有风险管理涵盖的三个完整阶段。德勤正不断努力使自身成为这样的一个企业，同时我们也有成熟的风险服务来帮助客户共同实现这一目标。

网络安全事件响应生命周期

虽然无法精确预测事件的性质、位置和影响，但是事件响应生命周期却遵循一个可预测的轨迹（见图2）。

网络安全事件响应生命周期（Cyber Incident Response Lifecycle，或简称“CIR生命周期”）显示出了企业能力和利益相关方信心之间的相互影响。当发生网络安全事件发生后，企业需要立即恢复受到影响的业务和运营能力。这通常需要几个小时或几天，在严重的情况下甚至可能需要几个星期，甚至几个月。此外，加强安全，也是为了保障运营环境的安全，提高对威胁可预测性，并减少对未来遭遇事件时的影响。

在危机处理过程中需要积极主动地消除利益相关方的担心，并控制事件的恶化。客户通常会特别关注个人资料和隐私信息的泄露问题，并可能对企业品牌和声誉产生长期的不信任。

商业伙伴一般会担心系统数据在当前是否会发生错乱，以及长久的数据和交易完整性。员工可能会受负面的宣传报道和过大压力影响而情绪低落。监管机构会要求保障消费者的利益，维护行业和市场稳定。投资者短期内比较关注遭受到的财务影响，而长期将更关注企业品牌和业务的活力与影响。

在CIR生命周期中，危机沟通是最重要的。具体而言，企业应该做到：

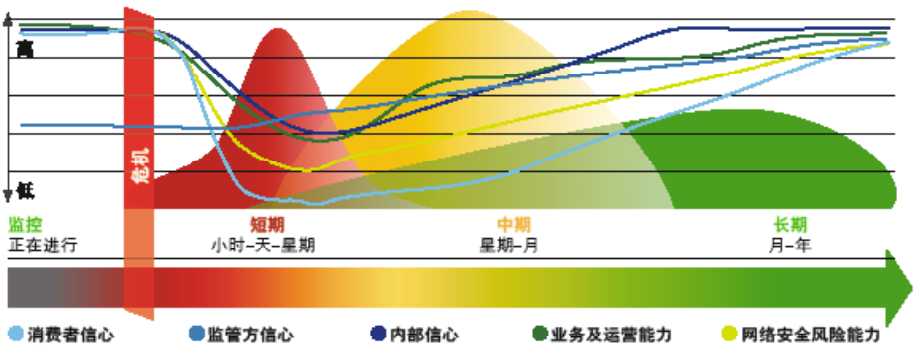
- 响应来自客户、商业伙伴、供应商、监管机构、执法部门和董事会的各类要求
- 处理来自商业伙伴的请求，并相应调整业务安排，工作步骤以及共享信息的方法
- 向利益相关方和公众广泛而积极地传递信息，包括他们已知和未知的情况，并告诉他们企业正在做些什么
- 对传统媒体、网络媒体以及社交媒体的舆论进行监测，了解他们对事件以及企业响应的评价与报道。

此外，管理层还应当：

- 处理法律或监管方面的潜在威胁，并确定企业可以使用哪些法律方面的资源
- 最大限度地缩短制定和实施缓解计划的时间间隔，并控制在这个时间差内所产生的风险

计划越是全面和经过有效测试，管理层对事件的响应就越会取得成功。然而，管理者应该明白，这样的计划并不代表一个剧本，并不是在计划中设计的步骤都会在现实中出现，企业的响应应该是灵活而又顺畅的。在真正响应危机时，您可能无法照搬整个计划，但计划将会提供一个框架和指导，协调参与响应的各个团队。

图2 事件响应生命周期



保持协调

事件响应程序需要企业在六个关键领域充分协调与实施——治理、战略、技术、商业运作、风险和合规性、以及纠正与改进。

1 治理

治理为企业管理危机响应与处理团队提供框架。它确保多个部门共同有序参与响应工作，规范了危机管理的政策、制度和流程，明确了危机沟通角色、职责、沟通方式和渠道。治理使危机响应策略与企业目标相一致，并提供跨职能团队的沟通机制。

建立危机响应治理的关键步骤包括：

- 实现职责分离，建立一个独立的调查小组来确定事件发生原因及后续的补救措施
- 明确法律顾问的角色，他应该参与或作为代表参与到危机响应小组，该小组应由业务经理领导，以促进 CIR 过程中的跨部门协同
- 明确事件响应和恢复生命周期阶段，定义清晰的决策框架，包括清晰的步骤的成功条件

关键问题

- 我们是否有合适的团队？
- 什么时候，向谁，汇报什么内容？
- 我们是否定期测试我们的计划和培训员工？
- 我们如何汲取经验教训？

图3 有效响应要求的跨部门能力

2 策略

响应策略定义了在事件响应和危机管理过程中，您应该如何指挥、领导、协调和沟通。企业应使响应策略与本企业的责任和价值观相一致。一个健全的策略会提供一种满足成本效益、资源充足、范围全面的方法来应对事件。这样在危机管理规划时可以最大限度地拓宽视野，有全局性的考虑，并减少对运营和收入的不利影响。

应对策略的关键环节包括：

- 定义升级和优先级排序方式来管理和协调 IT、运营和业务的恢复
- 企业的政府事务团队或其它府联络职能部门需要与监管机构和相关官员保持沟通与合作——这是受监管行业应该遵循的重要步骤
- 危机响应工作需要与安全管理和 IT 活动相一致

关键问题

- 什么时候应通知高级管理层和董事会?
- 我们的战略是否考虑了内外部的协调机制?
- 我们如何协助受影响的利益相关方?
- 最好的沟通渠道是什么?

3 技术

IT 和安全团队制定和实施相关机制，用于检测、监控、响应、并从事件或危机中恢复；IT 工程师开发所需的架构；IT 团队进行系统维护，抵抗攻击。

技术取证和调查能力对于保护证据、分析控制失效、安全漏洞以及其它与事件相关的情况是至关重要的（参见页 24：事件发生后：调查和响应）。此外，企业应实施可主动侦测和响应的技术解决方案，降低未来发生事件的可能性。

构建事件响应的技术方面时，关键步骤包括：

- 实际可操作的 IT 工具，它可以实现安全和保障运营性能，但是不会消除风险
- 解决事件发生后的紧急需求与长期补救措施之间的矛盾
- 经常需要接受变通方案以满足近期的优先事项

关键问题

- 我们采用哪种事件和危机的缓解技术?
- 我们有什么技术能力,我们又缺少什么?
- 我们是否有取证的资源?
- 我们如何收集和使用威胁情报

事件发生后：调查与响应

参照实际犯罪现场的模式，考虑数字犯罪现场：毁坏证据或清理痕迹会给法律取证增加难度。所以该小组应将确保数字犯罪现场和证据的完整保存作为第一步。

然而，拯救“受害者”——即被破坏的系统，可能需要运行某一流程或业务——当然这一流程或业务可能本身也是优先事项之一。这个意思是，恢复策略也要求“受害者”系统首先得到救援。在这种情况下，企业需要在恢复系统与保存证据之间做出权衡。

一般情况下，下列事件的处理步骤可以协助查明原因，进行补救并加快恢复：

- 记录这起事件是如何被发现的，谁报告该事件的，以及他们是如何知晓的；访谈 IT 人员及相关方
- 考虑和研究内部参与的可能性，并采取措施以控制风险扩大的趋势
- 确定受影响的系统并对其隔离，不要让人去试图解决、修补、或改变系统的状态
- 收集现有的所有证据并加以分析，以确定事件的原因、严重程度和影响
- 根据分析结果加强网络安全，提高协议的安全性，并增加警惕性
- 加强监控并采取其它措施，以减少未来类似事件的风险，并修订政策来增强安全
- 记录并向所有相关的利害关系者报告调查结果，并考虑潜在的向监管机构报告事件的要求

如果缺乏有效的调查响应，可能永远无法知晓该事件发生的真实原因，那么同类事件重复发生的可能性会增加。速度对于控制时间造成的损失至关重要。以保险为例，迅速响应可进行更准确地评估损失，确定索赔金额，并更快地获得理赔。

4  业务运营

事件发生后，关键业务运营必须尽快恢复，以使中断产生的财务、声誉、监管和利益相关者的影响最小化。

减小业务中断影响的关键包括：

- 在事件响应或恢复程序中，采取“带外”流程来替代被破坏或者受限制的流程
- 规划应对超出常规的支持请求，并分配相应的资源
- 了解现有的业务限制，例如使用标准支付系统或某些应用程序的风险

关键问题

- 哪些业务流程和应用系统对运营来说是最关键的？
- 哪些基础设施必须给予最大的保护？
- 我们将如何完全恢复到正常运营状态？
- 如何使员工、供应商和合作伙伴协同支持恢复工作？

5  风险与合规

风险与合规部门应评估和管理事件和危机响应的合规因素，包括与法律顾问、监管机构和执法部门的对接。重中之重就是符合要求并证明合规。例如，在事件发生后，必须记录调查及响应的整个流程，以证明调查和响应过程的充分性。

事件发生后，成功管理风险及合规的关键包括：

- 预见到来自监管和执法部门的要求，可能包括对系统访问的请求以及对响应活动的审阅
- 针对保险或其它报告要求分析事件的影响和损失
- 在事件响应过程中，充分理解由自发的程序和技术，以及工作变通带来的额外风险

关键问题

- 什么情况需要进行违规事件通知？
- 监管和第三方的责任是什么？
- 应在何时以及如何告知执法部门？
- 该特定事件（组）如何影响本企业的合规前景？

6  纠正与改进

纠正与改进阶段将在关键业务恢复后启动，通过长期与短期的努力来弥补缺陷。企业必须确认攻击途径或媒介已被消除，并采取措施以防止类似攻击的再次发生。

纠正与改进必须消除或最小化事故发生的根本原因，并将业务、职能、IT 以及利益相关者置于安全的运营环境之中。

成功纠正与改进的关键包括：

- 平衡数字资产保护与业务顺畅运作间的偏好
- 对众多技术项目和不断增长的 IT 预算需求进行优先级排序
- 为不断增加的监管审查和更加严格的监管要求做好准备

关键问题

- 有否找到影响 IT 及业务流程的根本原因？
- 纠正与改进计划是否制定？
- 根本原因是否已被消除或最小化？
- 教训是否已被汲取，如何学以致用？

应急响应小组应该包括来自上述六个方面的人员，形成一个充分、平衡和统一的方法，调动全企业的资源来应对的事件与危机。

危机管理中的五个教训

德勤在与企业高管进行危机管理工作时总结出如下经验：

1.准备工作无可替代

战争游戏、演练、以及其它结构化的准备工作，对于企业能否进行协调一致的响应至关重要。

2.每个决定都很重要

在危机中的每一个决定都可能放大企业声誉风险而影响利益相关者的利益，声誉风险具有比运营风险更迅速的破坏能力。

3.应在几分钟内快速响应

小组必须迅速做出响应，而不是在几小时或几天之后。他们必须控制事态、采取灵活的领导方式、在不明朗的情况下进行信息沟通并激励信心。

4.危机过去后仍需进行后续工作

危机过后，您必须采集数据，记录决策，管理财务，处理保险索赔，并满足法律法规要求。

5.您能变得更强

“多难兴邦”。几乎每一次危机都能为企业创造提升的机会，首先进行有效响应，然后伺机进行改善。

客户、供应商、员工和其他相关方应能体谅危机会偶尔到影响企业。但倘若企业管理不善，缺乏准备，应对不力，沟通混乱，就很难得到客户、供应商和相关方的理解。

您准备好了吗?

大多数企业自身缺乏应急响应和危机管理的资源和能力。特别因为专业知识更新、风险场景不断演化以及网络犯罪频发等因素，使得大多数企业很难仅凭借一己之力从容进行危机管理。因此，通过外包或合作的方式进行的安全和响应服务可能是企业最佳的选择。

根据网络威胁情报，如还可以通过与业内同行交流或聘请专家，对企业来说这些都是非常重要的。许多企业已在网络的监控和风险管理方面的开发和维护工作上得益于外部的支持。

举例来说，24/7 的实时监控可以提供网络威胁的早期预警，风险感知可以探测到犯罪活动的行为模式。但由于财务成本因素，大多数企业不可能自行研发这样的系统。出于同样的目的，通过危机模拟、战争游戏和其它评估方式，来验证应急响应和危机管理的准备情况、响应能力、恢复计划，可以发现这些计划中的差距和不足，但很多企业也缺乏这种能力。

谈到事件响应和危机管理，“准备就绪”是一个动态演化的状态。昨天您可能已“准备就绪”，但今天可能就无法阻止新的网络犯罪攻击。事实上，您确实无法预先获知下一次攻击的具体来源或目标。但可以根据数字资产价值和受损害的影响来权衡风险，您也评估可能性。您确实可以使企业准备好进行有效应对和恢复!

联络人

薛梓源
合伙人
风险咨询
电话：+86 10 8520 7315
电子邮箱：tonxue@deloitte.com.cn

何晓明
合伙人
风险咨询
电话：+86 10 8512 5312
电子邮箱：the@deloitte.com.cn

冯晔
合伙人
风险咨询
电话：+86 21 6141 1575
电子邮箱：stefeng@deloitte.com.cn

施建俊
合伙人
风险咨询
电话：+86 21 2316 6953
电子邮箱：alexshi@deloitte.com.cn

邓景山
合伙人
风险咨询
电话： +86 755 3353 8639
电子邮箱：tertang@deloitte.com.cn

郭仪雅
合伙人
风险咨询
电话：+852 2852 6304
电子邮箱：evakwok@deloitte.com.hk

李卓伟
合伙人
风险咨询
电话：+852 2852 1931
电子邮箱：thomalee@deloitte.com.hk

关于德勤全球

Deloitte（“德勤”）泛指一家或多家德勤有限公司（即根据英国法律组成的私人担保有限公司，以下称“德勤有限公司”），以及其成员所网络和它们的关联机构。德勤有限公司与其每一家成员所均为具有独立法律地位的法律实体。德勤有限公司（又称“德勤全球”）并不向客户提供服务。请参阅 www.deloitte.com/cn/about 中有关德勤有限公司及其成员所更为详细的描述。

德勤为各行各业的上市及非上市客户提供审计、企业管理咨询、财务咨询、风险管理、税务及相关服务。德勤透过遍及全球逾150个国家的成员所网络为财富全球500强企业中的80%企业提供专业服务。凭借其世界一流和高质量的专业服务，协助客户应对极为复杂的商业挑战。如欲进一步了解全球大约244,400名德勤专业人员如何致力成就不凡，欢迎浏览我们的Facebook、LinkedIn 或Twitter专页。

关于德勤大中华

作为其中一所具领导地位的专业服务事务所，我们在大中华设有24个办事处分布于北京、香港、上海、台北、长沙、成都、重庆、大连、广州、杭州、哈尔滨、合肥、新竹、济南、高雄、澳门、南京、深圳、苏州、台中、台南、天津、武汉和厦门。我们拥有近13,500名员工，按照当地适用法规以协作方式服务客户。

关于德勤中国

德勤于1917年在上海设立办事处，德勤品牌由此进入中国。如今，德勤中国的事务所网络在德勤全球网络的支持下，为中国本地和在华的跨国及高增长企业客户提供全面的审计、企业管理咨询、财务咨询、企业风险管理和税务服务。德勤在中国市场拥有丰富经验，同时致力在中国会计准则、税务制度及培养本地专业会计师方面的发展做出重要贡献。敬请访问 www2.deloitte.com/cn/zh/social-media ，通过德勤中国的社交媒体平台，了解德勤在中国市场成就不凡的更多信息。

CQ-060SC-16