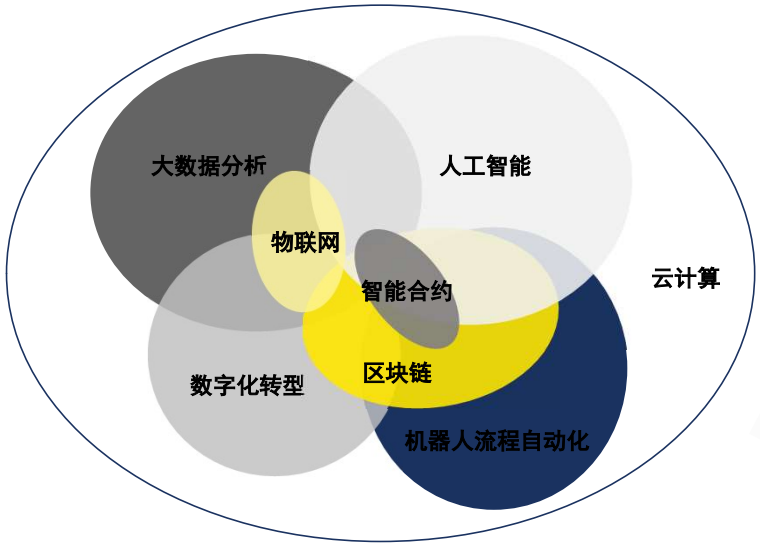
新形势下信息技术风险管理

刘强

2023年11月28日

新技术革新浪潮势不可挡，颠覆传统认知

- 互联网化
- 云计算
- 移动应用
- 大数据
- 机器人（包含RPA）
- 数字化
- 物联网
- 人工智能
- 区块链
- ……




工作、社交


购物、物流


交通出行


视频、游戏、AR

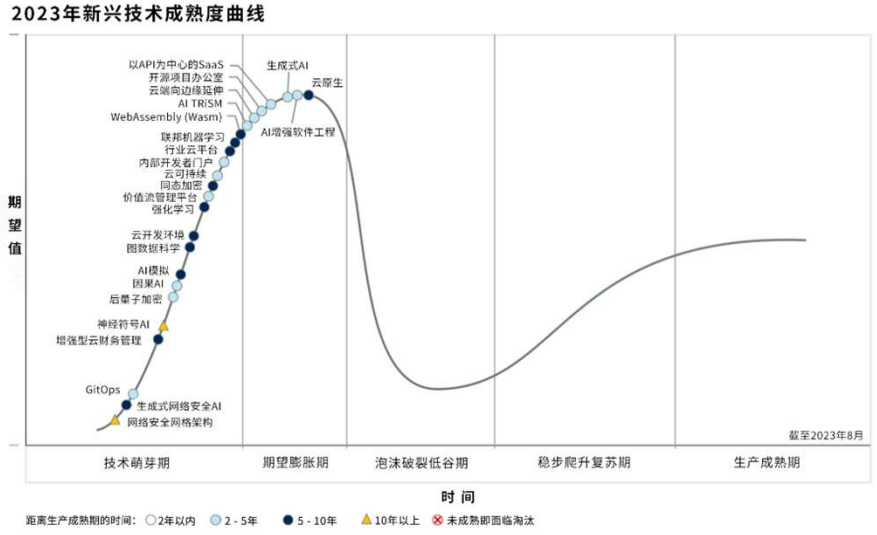

在线支付


机器人

GARTNER新技术趋势-2023

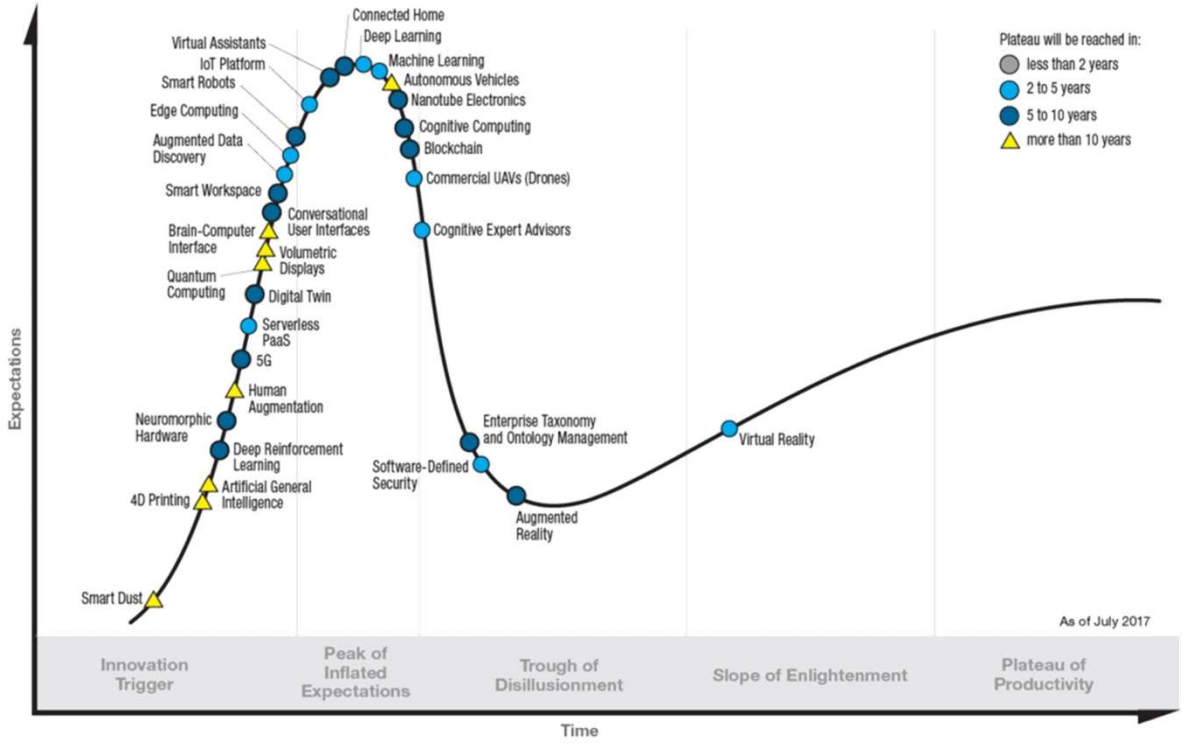
Gartner研究副总裁Melissa Davis表示：“这些技术都处于早期阶段，有些甚至还处于萌芽阶段，它们的未来发展存在很大的不确定性。对企业而言，部署尚在雏形期的技术具有很大风险，但同时也意味着更好的发展潜力。这些技术的早期采用者将获得不受限于Gartner重要战略技术**趋势**的差异化竞争力.”

2023年新兴技术成熟度曲线



来源：Gartner（2023年8月）

GARTNER新技术趋势-2017



IT风险事件案例

随着全球化、信息化的不断发展，物联网、云计算、大数据等新兴技术不断涌现，移动互联网也越来越渗入人们生活的各个方面，信息量呈爆炸式增长，各行各业面临的IT风险问题也越来越严峻。

滴滴违规被罚80.26亿元

- 2022年7月21日，滴滴因违法过度收集信息、存在严重影响国家安全的数据处理活动等，被处人民币**80.26亿元**罚款；

通信公司设备问题导致紧急呼叫无法拨出

- 美国第二大的电信公司T-Mobile无线服务出现长达12小时的设备故障，导致全国将**2.5亿个电话**及多个州的**2.3万个911紧急呼叫**无法接通；

- 2023年1月30日，厦门银行因泄露个人信息等23项违法行为被处罚款**764.6万元**的行政处罚。

厦门银行被开764.6万元大罚单

- 2020年2月23日，微盟集团某员工，登陆公司服务器后执行删除任务，将微盟服务器内数据全部删除；该事件导致次日开盘，公司市值蒸发超**6亿港元。**

微盟员工删库跑路致公司市值蒸发6亿

IT风险事件案例

希腊电信巨头遭黑客攻击，大量用户个人信息被泄露　　通信业 数据安全 隐私泄露

2020年10月，据外媒报道，希腊最大的电信网络公司Cosmote发生重大数据泄露事件，大量用户的个人信息遭泄露，可能会对“国家安全问题”产生重大影响。据报道，此次信息泄露是由国外黑客实施网络攻击造成的，黑客窃取了2020年9月1日至5日期间的电话等数据。

系统管理员利用职务之便篡改系统　　数据安全 监控管理

2018年6月4日14时许，韩某在位于北京市某地的链家公司，利用其担任数据库管理员并掌握公司财务系统root权限的便利，登录公司财务系统服务器，删除了财务数据及相关应用程序，导致链家EBS系统无法登录和服务不可用，无法进行财务月结。北京市海淀区人民法院认为，被告人韩某对计算机信息系统中存储的数据和应用程序进行删除，后果特别严重，其行为已构成破坏计算机信息系统罪，依法应予惩处。最终被告人韩某犯破坏计算机信息系统罪，判处有期徒刑七年。

IT风险事件案例

AI换脸应用引发隐私争议　　隐私保护 数据安全 科技伦理

2019年8月，一款AI换脸软件在社交媒体刷屏，但在用户协议上，存有很多陷阱，使用者的肖像权为“全球范围内免费、不可撤、永久可转授权”。而如果侵权了明星肖像，若对方提告，则最后责任都在用户。不合理的用户协议是AI换脸应用事件问题最严重的方面。相关的文字与诸多个人数据保护条例、人工智能伦理原则等都是相违背的。

自动驾驶安全事故频发　　自动驾驶 科技伦理

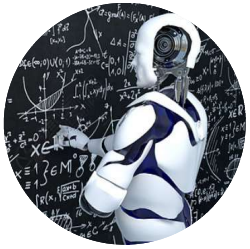
2019年4月17日，美国德克萨斯州，车主Micah Lee驾驶电动汽车时，突然撞到路边的大树引起爆燃，导致车主死亡，两名乘客受伤。调查该案件的警方认为，事故发生时这辆特斯拉正处于自动驾驶模式。根据美国国家公路交通安全管理局2022年7月份发布的 L2 级自动驾驶事故数据报告， 2021 年 7月1日至 2022 年 5 月15日的10个月内，有392 起事故与L2级ADS辅助驾驶系统有关。

IT新形势与当前技术趋势介绍

由于IT技术在各行各业中的普及和应用，以IT为主导的数字经济逐渐崛起，并对整个全球经济产生了巨大影响。IT行业的趋势和新技术持续更新，当前最新的IT技术主要有：

大数据应用

大数据指高速 (Velocity) 涌现的大量 (Volume) 多样化 (Variety) 数据，商业领域是大数据应用最广泛的领域之一。大数据可以帮助企业实现数据驱动的商业决策，包括市场营销、客户关系管理、产品研发等。企业可以通过收集、分析和利用大数据制定更加有效的商业战略。



人工智能和机器学习

人工智能与机器学习通过自动化测试和模型构建，可以更快速地进行数据筛选、异常检测和模式识别，提供智能化的建议和决策支持，为现有的商业智能工具添加更多的智能和洞察力。

人工智能生成内容（AIGC）

AIGC模型可以通过对信息系统数据的深度分析和模式识别。它的核心思想是利用人工智能模型，根据给定的主题、关键词、格式、风格等条件，自动生成各种类型的文本、图像、音频、视频等内容。AIGC可以广泛应用于各个领域，为用户提供高质量、高效率、高个性化的内容服务。

云计算和数据安全

云计算是一种将计算资源和服务通过互联网提供给用户使用的模式。这种模式下企业的数据和应用程序不再只存在于本地，而是分布在全球的多个数据中心。这种分布性使得数据和应用程序更容易受到攻击。

元宇宙

元宇宙是人类运用数字技术构建的，由现实世界映射或超越现实世界，可与现实世界交互的虚拟世界，具备新型社会体系的数字生活空间。元宇宙本身并不是新技术，而是集成了一大批现有技术，包括5G、云计算、人工智能、虚拟现实、区块链、数字货币、物联网、人机交互等。

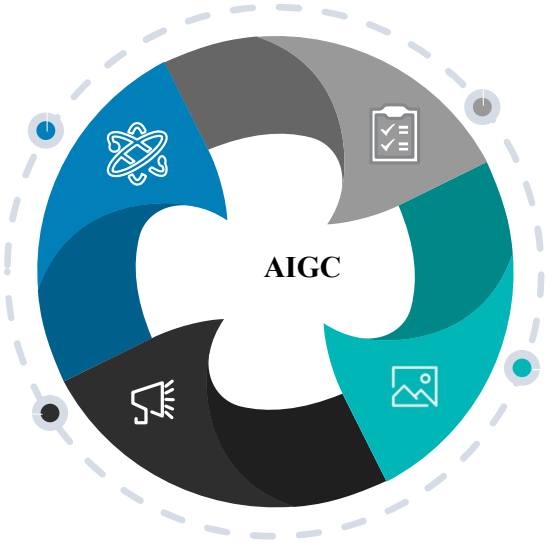
人工智能生成内容（AIGC）

自动生成代码

Amazon CodeWhisperer
CODEBOTS
tabnine
OpenAI Codex

自动合成语音

Thundercontent
Microsoft
Play.ht
Cleanvoice



和人类流畅交流

cohere
BLOOM
DeepMind
Character.AI
AI21labs
HyperWrite
Otter.ai

根据描述生成视频和图像

MODELPLACE
stability.ai
Midjourney
Point E
DALL·E 2
LUMA AI
NVIDIA

参考资料：1. What is generative AI? 》，麦肯锡；2. What Is Artificial Intelligence (AI) | Gartner，Gartner；3.《Generative AI 》，波士顿咨询公司；4. TE智库《企业AIGC商业落地应用研究报告》，TE智库AIGC企服指数

AIGC：Artificial Intelligence Generated Context，即可以利用人工智能技术自动产生内容，常见如代码生成、图片生成、文本问答等。

麦肯锡：生成式人工智能旨在通过以一种接近人类行为，（与人类）进行交互式协作。[1]

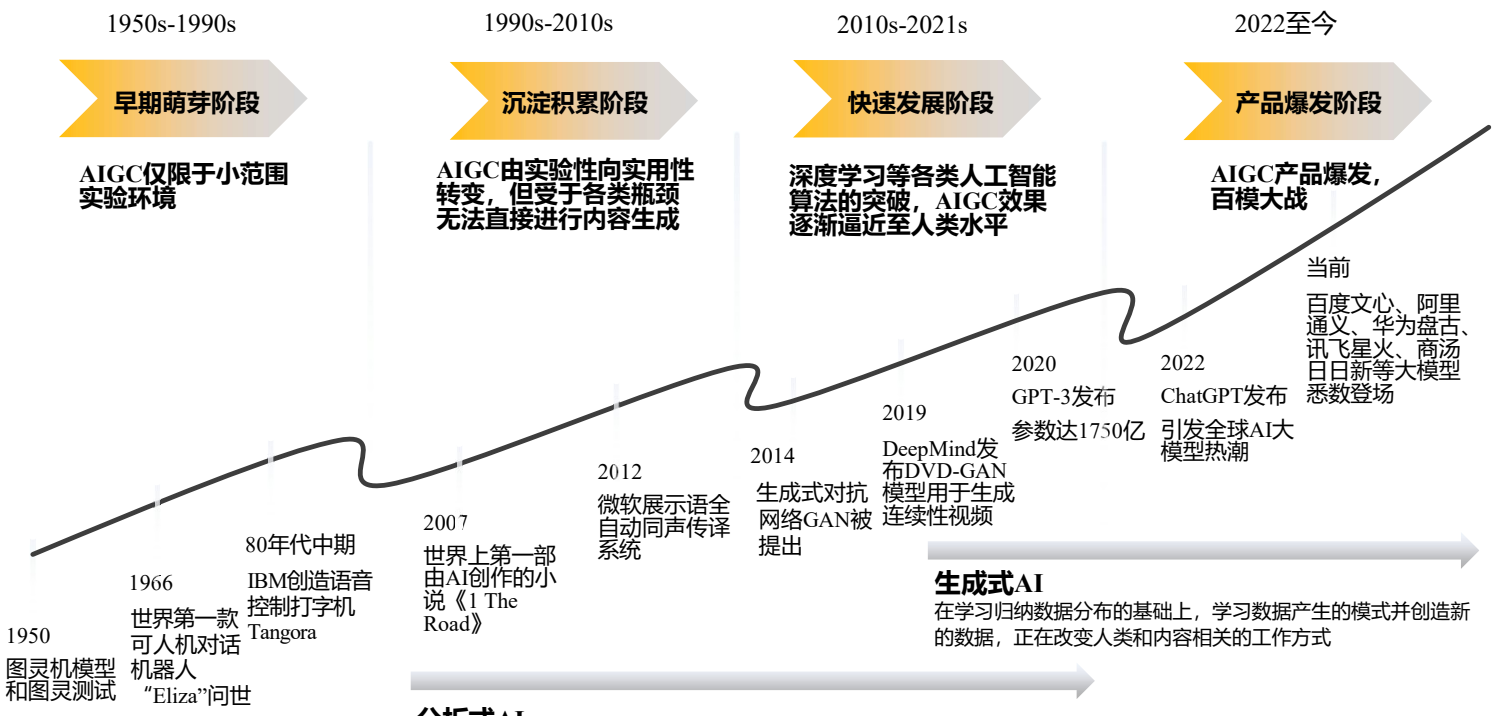
Gartner：生成式人工智能是一种颠覆性的技术，它可以生成以前依赖于人类的工件，在没有人类经验和思维过程偏见的情况下提供创新的结果。[2]

BCG：生成式AI是一种突破性的人工智能形式，它使用对抗网络(GANs)的深度学习技术来创建新颖的内容。[3]

TE智库：生成式人工智能，将彻底改变人机交互的关系，并创造新的产能输出结构。它将在第四维度实现与人的思维同调，类似移动设备以人类外器官形态存在，AIGC将以外脑的形式存在于人类认知中。[4]

人工智能生成内容（AIGC）

AIGC发展历程



AIGC带来的风险

- 数据安全
  - 数据全生命周期的安全
  - 数据跨境传输
  - 隐私保护
- 内生安全
  - 算法安全
  - 模型安全
  - 协同引发的内生安全
  - 运行环境引发的内生安全
- 内容安全
  - 生成制作非法内容
  - 生成内容被非法利用
- 其他
  - 可解释性问题
  - 伦理问题
  - 碳排放问题
  - 版权问题

国内人工智能安全合规法规与标准最新进展

- 2018年《具有舆论属性或社会动员能力的互联网信息服务安全评估规定》
- 2022年《互联网信息服务算法推荐管理规定》
- 2022年《移动互联网应用程序信息服务管理规定》
- 2023年《生成式人工智能服务管理办法（征求意见稿）》
- 2023年《生成式人工智能服务管理暂行办法》
- 2023年《GB/T 42888 信息安全技术 机器学习算法安全评估规范》

人工智能

人工智能通常被定义为学习、理解、识别人类语言、解决问题等能力的机器或软件。AI可以通过两种主要的方式展现这些能力：通过预编程规则来处理信息，或者使用一种叫做“机器学习”的技术从数据或其环境中学习。

在深度学习，一种特殊类型的机器学习的驱动下，人工智能已经在许多领域取得了重大的突破。例如，人工智能现在可以识别图像和语音、生成真实的人类语言、预测疾病的发展等等。

风险关注点

算法公平性

- 审计应检查算法的公平性，以确保所有用户都能公平地受益于人工智能系统。

透明度和可解释性

- 审计应评估系统的透明度和可解释性，以增强用户的信任和接受度。

可控、合规和持续监控

- 审计应检查系统的安全措施和隐私保护策略。
- 人工智能系统需要持续地进行监控和更新，以应对环境的变化和新出现的风险。审计应检查系统的监控和更新机制。

云计算

云计算使企业能够摆脱复杂的内部信息技术结构，允许企业专注于战略而非运营，并能快速地回应不断变化的市场条件。由于云计算能提供便捷、灵活的网络连接至可配置的资源共享池（例如：网络、服务器、存储、应用软件和服务），这些资源共享池只需要少量的管理或服务提供商的支援，就能迅速地提供服务。云计算技术正在快速发展，为企业提供不同选择。然而，跟大多数科技发展一样，云计算也有其风险和挑战，这些风险往往被忽视或不被理解。

风险关注点

云战略和治理

- 评估企业的云战略是否与业务目标一致

云安全和隐私

- 评估云提供商的信息安全操作和程序

云提供商服务

- 评估云提供商实践合同的能力、应急计划和扩展支持

网络安全

对网络安全的威胁一直在演变和无限制的增长，似乎任何人都会不经意地受到攻击。黑客们不再需要透过实体访问进入设施以对企业造成伤害。如今，他们可以通过恶意软件或网络钓鱼攻击、甚至连接第三方、新技术或者其他不断发展的途径，进入企业的设施。

各企业必须关注信息技术和信息安全，以避免成为网络威胁的受害者。同时，企业可以设定一个网络审计的程序，概括下列的范围：

安全意识：	评估对用户培训的流程和控制点，以提高他们对未经许可即进入企业的资讯以及系统的实体访问和逻辑访问的警觉以及敏感度。
资产管理：	评估有关连接企业网络的科技资产库存的流程和控制点。
供应商风险管理：	评估第三方服务商和供应商的流程和控制点。
事件反应：	评估管理层对检测到异常活动时的反应、流程和控制点。

元宇宙

元宇宙的出现将改变人们的信息交流方式，移动通讯网络作为连接现实世界与虚拟世界的重要桥梁，将会发挥更加重要的作用

风险关注点

由于元宇宙是一个新兴技术领域，相关的技术和标准仍在不断发展和完善中，这将对审计技术的选择和应用带来一定的风险。技术的更新和升级可能会对旧有的审计系统产生冲击，导致数据丢失或技术故障等问题。

元宇宙中的活动和交易涉及到法律和监管问题，例如虚拟货币的交易、知识产权的保护等。如果审计人员对相关法律和监管要求不了解或不重视，可能会引发法律风险和合规问题。

作为一个全新的技术领域，内部审计人员需要加强自身的技术学习和专业素养，同时加强与相关方面的沟通和协作，加强对数据安全和法律风险的防范和管理，以确保审计工作的准确性和有效性。

元宇宙合规审计

- 检查元宇宙平台是否符合相关法律法规和监管要求

元宇宙安全审计

- 评估元宇宙中的数据安全性、网络安全性及用户隐私保护控制

谢谢大家！

SAM.Q.LIU@CN.EY.COM