1．策略建议

云服务提供商应该为那些在安全方面要求严格的客户建立一个安全基线(内容可包括系统，设施和流程等)。这些安全指南不应给客户体验带来负面的影响，严格的安全指南应该是经济的，并且可以有效地降低企业人员、公司收入、声誉和股东价值等方面所面对的风险。

另外，云服务提供商也要为低安全需求的用户建立安全基线，或者为所有用户提供一个基线，在此基础上为那些有需求的用户提供更多的附加服务选项。对于后一种情况，提供商应该意识到有些客户只对那些仅提供高安全等级服务的服务商有兴趣。服务商必须在系统，设施和流程等方面就安全等级进行权衡。

云服务提供商应该严格划分工作职责，实行背景调查，要求并强制员工签署保密协议，并基于最小权限原则限制员工获取客户的信息。

2．透明性建议

为了表明在安全方面的态度，云服务提供商需要提高服务的透明度。现场参观云服务提供商的设施和数据中心可以帮助用户更好地评估服务水平，清楚地理解各种安全标准。但是，云计算具有按需置备和多租户等特性，传统形式的审计和评估可能不适用，或者需要修改(如共享式访问与第三方检查)。

为了增加现场评估的效力，应该在没有事先通知的情况下（如果需要事先通知，指定一个较宽泛的时间窗口而不是一个特定的时间）拜访云服务提供商的设施或数据中心。这样可以保障用户在一个平常的工作日里进行一次真实的评估，而不是由云服务提供商在客户或第三方访问时装装门面。

如果需要直接检查，评估团队应该由两名或更多来自 IT、信息安全、业务连续性、物理安全和管理部门（如部门首脑或数据所有者）的专家组成。

在访问之前，客户应该索取业务连续性计划和灾难恢复文档，包括相关的证书（基于 ISO，ITIL 等标准），审计报告和测试协议。

3．人力资源建议

客户应该检查云服务提供商是否为保障物理安全而部署了能胜任工作的安全人员。建议配置一名负责领导和推动物理安全项目的专职安全经理。业界顶尖的认证可以帮助你验证工作人员在物理安全方面的知 识和技能，例如 CISA，CISSP，CISM，ITIL，或者 CPP(from ASIS)。

客户应该索取一份全面介绍安全经理及其组织的报告。它可以帮助你判断该位置上是否安排了尽职尽责的人员。安全经理应该向部门主管或 GRC 委员会报告，而不是向物业或 IT 人员报告。为了保证这一职位的独立与客观，最好可以通过其他途径（如通过 CRO 或公司高管）向 CEO 报告。

4．业务连续性建议

已部署服务的连续性通常由第三方在合约中做出承诺，客户只需要审查合约，但实际上

客户才是实际的数据管理者，因此有必要对服务商的能力做深入的分析。对于个人数据，通常要遵循特定的法规要求，采取相应的控制手段。即使采用第三方数据处理服务也是如此。

客户应该审查第三方的业务连续性流程和特定的认证。例如，云服务提供商可能取得了BS25999，即业务连续性管理英国标准。客户可以审查这一认证的范围和评估细节记录。

客户应该对云服务提供商的设施进行现场评估，以确认和验证服务商为保证服务的连续性所采取的控制手段。如果要检验特定业务连续性计划的实现，一般不应采取这种不事先通告的服务商设施评估，因为这一类实现只有在灾难或事件发生时才会被启用。

客户要保证自己在云服务提供商执行完任何的业务连续性计划或灾难恢复计划测试之后都能收到确认。要特别关注的是，服务商确实是通过模拟重大事件发生来进行测试的，并通过文档承诺服务的可用性 得到保障。这在许多的建议中都曾经提到过。客户应该对业务连续性和灾难恢复测试的正式报告给予特 别重视，要清楚地了解测试是否满足合约中所承诺的服务级别。不要等待灾难真的发生时才重视。

5．灾难恢复建议

使用云服务的客户不应依赖单一服务商的服务，应该制定一个灾难恢复计划，明确当前服务商失去服务能力时，如何对业务系统进行迁移或故障切换。

- 基础架构云服务商应该在合约中约定，采用多种平台来提供服务，且必须拥有在服务受损之后可用于快速恢复系统的工具。
- 数据验证应该是一个自动化的，或者基于可由用户启动的验证协议，以便客户可以随时检查他们的数据，从而确保数据的完整性。
- 增量备份可以按照系统用户所设定的间隔为所有受保护系统或快照更新副本。消费者可以根据恢复点目标来决定设置。
- 可以通过一个用户驱动的，自助服务的门户来访问全站、系统、磁盘和文件恢复服务，这样用户就可以灵活地选择他们想要恢复哪个文件、磁盘或者系统。
- 云服务提供商应该提供快速的，符合服务等级协议的数据恢复服务。
- 服务等级协议应该预先协商好，客户只需要购买他们所需要的服务。所有的数据、文件或系统都应该在 30 min 以内恢复。
- 客户与物理站点之间的应该采用广域网优化技术，在确保数据可移动性的同时还可以减少带宽和存储设备的利用率，从而节省成本。