《网络安全审查办法（修订草案征求意见稿）》下应如何提升企业网络安全内部控制

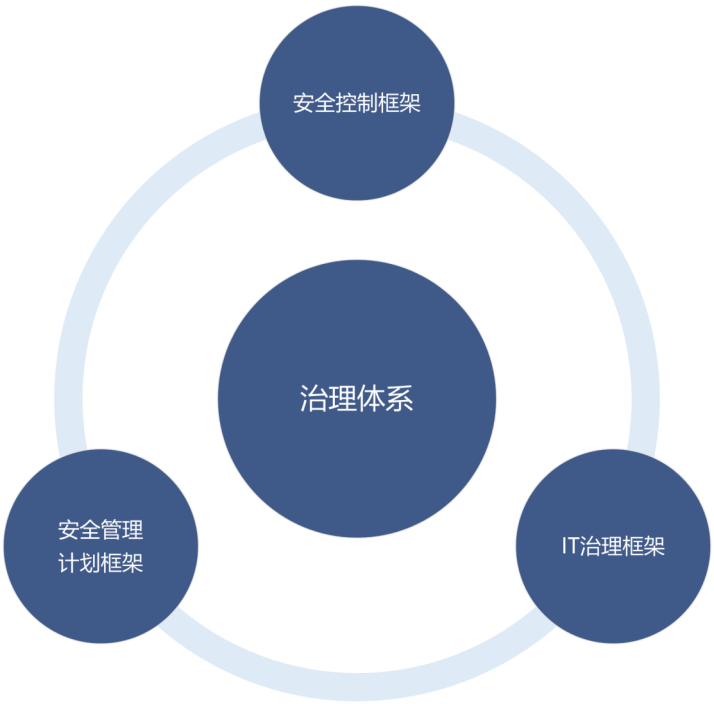
© AVISTA Group. All rights reserved.

本文包含的信息由艾华迪从可信的来源获取、整合所得，文中一切观点、分析和预期等均基于此类信息。尽管我们已尽力确保本文的准确性，艾华迪或任何其他人并不作声明或保证其准确性或完整性。本文中表达的所有意见和估计如有更改，恕不另行通知。本文受版权保护，未经艾华迪的书面许可，严禁以任何形式复制本文全部或部分信息内容。

前言

新型冠状病毒让大众居家防疫、企业推行在家办公，推进了资讯科技行业急速发展，线上游戏、通讯交流软件、电商等均是新冠疫情下的赢家。而各行业亦加速转型，采用更多大数据、云端计算及人工智能科技于日常运营。但是，应用新科技所带来的网络安全、数据安全及个人信息安全风险却越见重大。2021 年 7 月初，国家互联网信息办公室发布《网络安全审查办法（修订草案征求意见稿）》（「征求意见稿」）对近期中国境内公司申请国外上市所引发的数据安全担忧作出回应。随着各种法规的出台，企业应提高对网络安全、数据安全及用户个人信息保护的关注，加强内控系统，以免触犯法规而对企业营运带来严重影响。

企业资讯科技治理体系



© AVISTA Group. All rights reserved.

网络安全

互联网是常见的商业讯息交换渠道。互联网的连接带来了外部攻击者可能从外部侵入企业网络的网络安全风险。为减低相关风险，企业应采取以下主要的内控措施:

1. 制定网络风险管理政策

网络风险管理政策是重要文件，阐明管理层对网络安全风险管理方面的安全要求、程序和态度。管理层应建立健全机制、定期维护和宣传安全政策，以及向员工提供持续教育及培训。同时，为了确保政策符合法律法规，政策需根据监管要求及发展趋势及时更新和优化网络安全策略、制度、流程和规范。否则，在缺乏管理政策的情况下，员工可能因无章可循，以及对法例法规的不熟悉以致出现不合规事故。除按照法律法规的要求外，企业于制订政策时可参考三类安全框架，包括安全控制框架 (如： ISO27002, CIS 20)、安全管理计划框架 (如：ISO 27001, NIST CSF) 及 IT 治理框架 (如： COBIT 2019, ITIL) 。

- 安全控制框架为企业提供综合控制点列表，其中 CIS 20 列出了 20 项安全控制，当中分为基础 (6 项) 、进阶安全基准 (10 项) 、企业组织 (4 项) ，从而协助企业有效设计、构建及维护系统及网络之安全流程。
- 资讯安全管理系统，是一套有系统分析和管理资讯系统的方法，其中 CSF 框架涵盖了资讯安全的 5 大面向，包括识别、保护、侦测、回应与复原，并针对不同范畴如供应链安全、身份识别与验证，以及自我评估资讯安全风险提供了指引，使企业能建立网络安全生命周期的风险管理。
- IT 治理框架提供了组织在组织内实施、管理和监控 IT 治理的方式和方法，并给予有效利用 IT 资源的建议和措施。其中 COBIT 2019 框架详细描述 40 个治理/管理目标，这些目标依据相关流程、企业目标以及治理和管理实务进行定义，且与之一致。

2. 委任资讯安全总监

面对日趋严紧的外部监管环境，企业需要在网络安全合规方面投入更多的资源。企业应加大网络安全研发投入和队伍建设，指派具相关专业知识的人员担任首席资讯安全总监以制订安全战略、措施和安全标准。不断推进网络安全技术研发和创新，并持续推动网络安全能力升级。

首席安全官负责整个机构的安全运行状态，包括信息技术、人力资源、通信、合规性及设备管理。

根据征求意见稿第 34 条，企业应当按照国家法律法规的规定和相关国家标准的要求，设置专门的网络安全管理机构和网络安全管理负责人，对网络安全管理负责人和关键岗位的人员进行安全背景审查，签署特殊保密协议，落实持证上岗制度。因此，企业亦应参照以上法律法规对各候选人进行充分的背景调查。

背景调查除包括法律法规所提到的安全背景审查外，企业亦应订立所需专业资格之标准，包括但不限于国际信息安全专家 (CISSP) 及注册信息安全管理员 (CISP) 等，确保候选人的专业及能力合乎职位之要求，并能有效降低网络风险。

© AVISTA Group. All rights reserved.

3. 网络安全测试

企业应定期进行网络安全测试，包括进行渗透测试及漏洞评估，以了解企业网络安全控制的风险和成熟度，并编制一个可行、符合成本效益的路线图来应对日益增长的网络风险。渗透测试工作往往作为风险评估的一个重要环节，为风险评估提供重要的原始参考数据。渗透测试是由具备高技能和高素质的安全服务人员发起、并利用常见的黑客攻击手段对目标系统进行模拟入侵，目的在于充分挖掘系统的弱点，从而让管理人员了解系统有可能面临的威胁。渗透测试的优点在于不但能在未知系统中发现弱点，而且能验证部分高危险性的弱点，甚至还能挖掘出一些未知的弱点。

4. 定期进行网络风险评估及制定紧急应变方案

企业应定期进行网络风险评估，并覆检资讯系统/ 网络设备的记录和审计追踪记录，透过建立自动化分析系统，以监测系统运作是否存在异常情况和可能出现的攻击。制订紧急应变方案（包括怀疑被入侵的事故程序），以确保遇到网络保安事故时也能即时作出应变。

根据《网络安全法》第 22 条及第 34 条、《关键信息基础设施安全保护条例（征求意见稿）》第 24 条，企业应当制定网络安全事件应急预案并定期进行演练；当企业发现提供的产品、服务存在安全缺陷、漏洞等风险时，应当立即采取补救措施，按照规定及时向主管部门报告。因此，企业亦应参照以上法律法规定期进行网络风险评估，否则，因系统漏洞造成网络安全事故，违背网络安全法，直接责任人和主管责任人将会按照网络安全法依法处罚，甚至造成经济和名誉的损失。

5. 安全意识培训

网络安全是每个员工均有的责任，企业可透过各种网络安全培训确保各员工了解安全风险，如企业网络安全治理、网络威胁、移动安全、云安全，以及信息保护和隐私意识等。

企业的安全意识培训可包含以下内容：

- 不同形式的网络安全威胁
- 密码安全的重要性
- 保护公司数据
- 如何识别和报告网络安全威胁

© AVISTA Group. All rights reserved.

数据安全

当前大量机构积极开展数字化战略，并利用大数据、人工智能及云计算等IT科技构建商业运营模式。随着数字化的重要性，业务上下游数据流转、汇集、对数据完整性、保密性和可用性提出更多安全方面的管理提升需求，企业应采取以下主要的内控措施:

1. 数据安全管理规划

企业于进行数据资产安全盘点及数据安全风险评估及消除后，应按照结果进行数据安全管理规划。企业应分别建立安全组织、规章制度及技术架构：

- 在合规或 IT 部门成立专业化数据安全团队，通过与数据治理组织的协同配合，保证能长期持续执行数据安全管理工作。
- 建立整体方针政策，加强数据资产分级分类和管控，划分敏感数据使用部门和人员角色，限定角色的数据使用场景，制定场景对应制度规范、操作标准和模板，推动执行落地。
- 规划数据安全技术架构，保护计算单元、存储设备、操作系统、应用程序和网络边界各层免受恶意软件、黑客入侵和内部人员窃取等威胁。

2. 数据资产安全盘点

数据安全对象的识别一般可以通过数据资产盘点的方式进行。我们建议数据资产的安全盘点要遵循外部法律、法规的合规要求实施，盘点过程中需要特别注意对个人隐私信息和重要数据的定义。数据资产安全盘点的产出是将期望识别的安全对象的关键属性与现有系统字段建立映射，具体的映射过程可以在信息系统的数据字典设计阶段进行。

在进行数据资产安全盘点时，企业应侧重于数据资产分级分类，分类步骤如下：

- 数据资产分类依据数据来源、内容和用途，划分相应数据机密级别。
- 识别核心数据资产，投入更多资源精细化管理数据安全，使数据安全在快捷共享和安全可控之间达到平衡。
- 对于敏感数据资产，按其所有者进行密级分类，将数据资产分级为公开、内部、敏感、机密等。

© AVISTA Group. All rights reserved.

3. 数据安全风险评估及消除

数据安全风险评估一般分为“按数据生命周期安全评估”和“按场景化数据安全评估”两种方法。将评估结果输入数据安全风险矩阵，输出风险视图和消除举措。

- 数据生命周期安全评估法

数据生命周期分为五大阶段，即数据采集、数据传输、数据储存、数据交换及数据销毁。企业应围绕以上各阶段，明确相关数据安全过程的监管法规要求和业务需求，分析及制定对应安全策略，从组织建设、制度流程、技术工具和人员能力角度评估数据安全现状。

- 场景化数据安全评估法

企业应围绕数据安全场景，以数据分级分类为核心，根据数据安全合规监管和业务提升要求，评估相应数据访问控制的现状差距、制定数据安全控制措施。当中的主要侧重点包括：用户权限管理、数据共享（提取）权限管理、定期权限稽核及数据存储管理。

除此之外，企业亦应注意数据管理时之法律法规事宜，避免出现不合规事故。根据《网络安全法》第 36 条，当境外执法、司法机构依据其职权对企业进行调查，要求企业提供相关数据时，企业不能径直按照境外执法机构的要求提供，应当先向主管部门报备方可提供。我们建议企业如收到任何由境外执法、司法机构的要求，所有员工应先通知管理层，及向相关执法、司法部门提取证明文件，保障数据安全。

个人信息安全

执法及司法部门于近年不断提高对个人信息安全的要求，并完善相关的法例法规、加强执法力度。因此，企业应采取以下主要的内控措施尽早增强维护个人信息的力度:

1. 计划与资讯搜集

如企业曾经或即将搜集用户之个人资讯，企业应尽快盘点已搜集、使用、存储的个人资讯类型、个人资讯对应的容器和载体、内部访问、处理、分析、使用这些个人资讯对应的人员岗位、存储这些个人资讯的资讯系统情况（例如系统后台资料库的物理位置等）、这些个人资讯有可能会被内部人员披露、传输予外部供应商。

2. 审阅信息处理现状

企业应详细审阅信息处理的各个操作步骤，包括但不限于收集、使用、存储、销毁、分享予第三方。

- 收集：有否于搜集个人信息前获取授权
- 使用：有否订立访问、查询、修改个人资讯之权限
- 存储：存储个人资讯的位置是否安全
- 销毁：包含个人资讯的文件是否于安全的办法及合理的时间点执行销毁
- 分享予第三方：有否于分享前获得授权及有否进行加密

3. 除以上内控措施外，企业亦应注意以下法例法规，避免出现任何不合规事宜。

- 根据《常见类型移动互联网应用程序必要个人信息范围规定》，企业不得因用户不同意提供非必要个人信息，而拒绝用户使用其基本功能。因此，企业应按照上述之步骤进行审阅。

- 根据征求意见稿，如企业掌握超过一百万用户个人信息，并计划前往国外上市，企业必须向网络安全审查办公室申报网络安全审查，并且网络安全审查主要考量的风险。 因此，如企业持有大量个人信息及计划前往国外上市，企业应时刻留意法律法规的更改及调整。

© AVISTA Group. All rights reserved.

数据出境安全

为降低数据出境的安全风险，执法及司法机构已细化和加强相关法律法规之内容及力度。现时与数据出境有关的法律法规包括但不限于：《网络安全法》、《个人信息保护法（草案二次审议稿）》、《数据安全法》、《个人信息和重要数据出境安全评估办法（征求意见稿）》、《信息安全技术数据出境安全评估指南（征求意见稿）》及《个人信息出境安全评估办法（征求意见稿）》。上述的法律法规中，《网络安全法》及《数据安全法》为已生效的法律法规，其他的则尚未生效，但可作为参考性质。

企业如决定于国外上市，应先执行上文提到之网络安全、数据安全及个人信息安全的内控措施，如数据盘点，风险评估等。另外，由于执法及司法机构已计划优化现时的法律法规，因此，企业应注意有关法律法规的更新。

结语

当今动态数位世界的新技术，如云计算，物联网和互联供应链，带来新的不确定性，满足监管要求也变得更加复杂。因此，企业可参考上述所提到的内部控制措施，甚至聘请第三方协助审视与构建 IT 治理体系，并通过 ISO 27001 验证，以向客户，员工和其他第三方发出明确信息，表明企业拥有严格及国际公认的信息安全实践及对资讯安全的承诺。

点击“**阅读原文**”，查阅国家互联网信息办公室关于征求意见稿公开征求意见的通知。

联系我们

彭颂邦

特许金融分析师，资深会计师(香港)，资深会计师(澳洲)，
皇家特许测量师学会专业会员，皇家特许测量师学会注册估价师

董事总经理

+852 3702 7338

vincent.pang@avaval.com

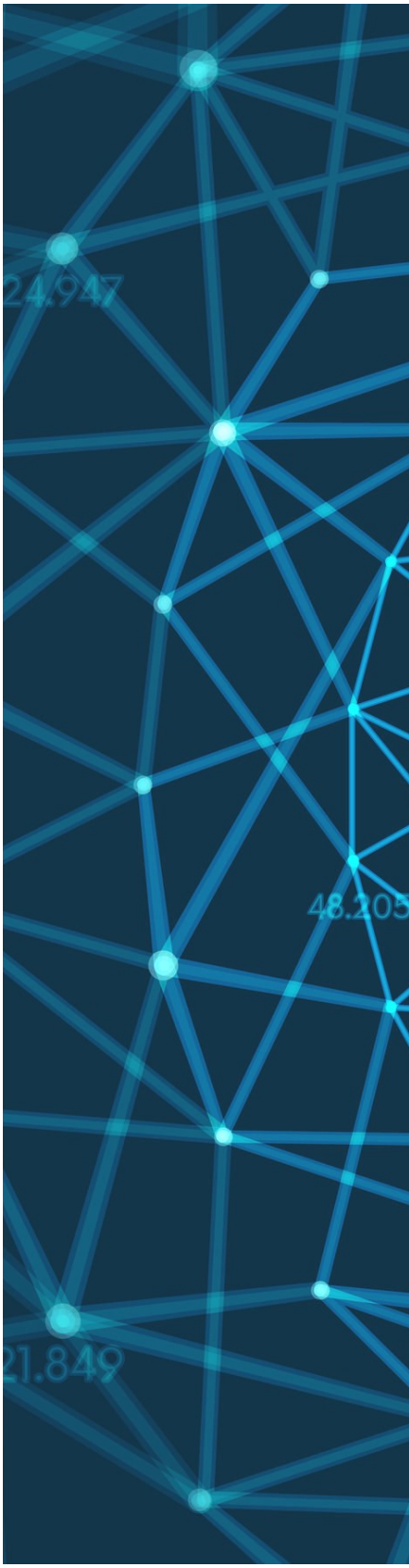
何焯维

会计师，英国特许公认会计师公会资深会员，国际注册内部审计师，
资讯系统审计师，注册税务顾问(香港)

董事, 风险管理咨询服务

+852 3702 7317

ricky.ho@avaval.com



© AVISTA Group. All rights reserved.