为了让 IT 环境适应整个企业发展的需要，企业通常会实施与其战略目标相一致的 IT 规划，这其中，作为有效防范和化解 IT 风险，并保证信息系统平稳运行和业务持续开展的重要环节，信息安全发展规划尤其重要。从整体来看，信息安全发展规划，既要遵循 IT 规划的框架和模式，又要充分考虑信息安全的特殊性，是一项专业要求非常高的工作。安言咨询经历在银行、电力、通讯、重点企业等领域长期的实践，积累了丰富的经验，总结并构建了一套成熟的信息安全规划方法和实施框架，并借此为有意通过整体规划来推动信息安全稳健发展的企业提供帮助。

安言咨询信息安全及 IT 风险管理整体解决方案

安言咨询风险管理框架采用 ISO 31000:2009《风险管理—原则与指南》国际标准，作为实施风险评估的主要标准依据。针对**安全策略层面、安全管理层面、组织结构和管理制度层面和信息安全技术**四个方面提供全面的风险评估过程，识别、分析和处置相关风险，形成综合性信息科技风险管理框架。

风险评估是信息安全管理体系（ISMS）建设一项非常重要的活动，基于企业信息安全风险评估的结果，项目组可以更加深入地阐明企业信息安全管理现状，以及企业业务运营的特定环境中存在的信息安全隐患。通过对潜在信息安全风险进行量化分解和描述，以数字化的形式展现风险发生时的影响范围和发生的可能性，进而帮助客户确定信息安全管理建设的详细需求和风险处置的投资成本收益。

安言咨询以在信息安全管理咨询领域中的长期实践为依据对企业信息安全的风险评估

提出下述实施要点，从而最大限度的确保风险评估成果最大化，实施要点如下：

- **业务流程、信息资产、合规并重。**仅基于业务流程的风险评估往往由于业务流程贯穿组织的众多部门而导致引起风险的原因不明确，处置风险的责任不清晰；而基于信息资产的风险评估又通常独立于业务环境而无法真实的反映企业的业务需求，仅按照固定资产的责任和归属进行风险管理和处置，导致治表而不治本。单方面的评估方法都不能适应企业业务发展和风险管控的要求，因此，安言将采用全新的，将业务流程、信息资产、合规融合的风险评估方法来解决业务流程运行过程中起关键和主导作用的信息资产所面临的信息科技风险；

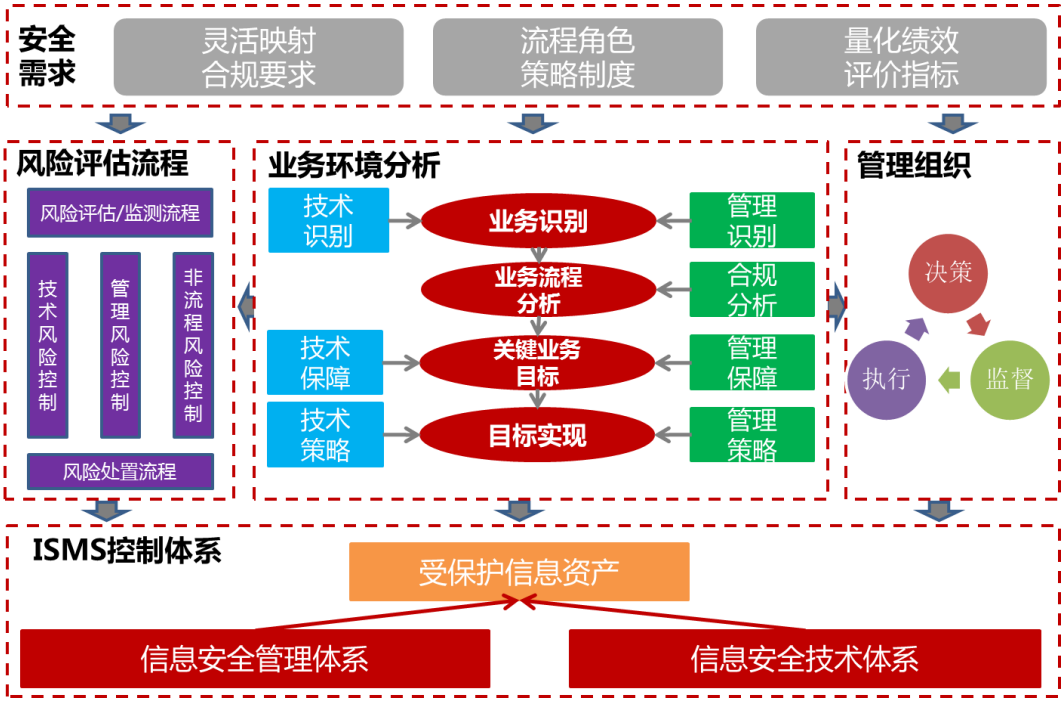
- **强调特定业务环境中的风险来源和识别。**业务流程和信息资产在企业的业务运作中都是静态资产，只有将两者纳入到特定的业务环境才能发现他们对于业务的支撑作用，安言咨询的 ISO/IEC /IEC 31000:2009 风险评估方法在识别业务流程和信息资产的基础上，创新的加入了对业务环境和风险源的识别，从而使特定业务环境成为立体的、可见的风险控制模块，同时在此基础上，通过识别业务流程和信息资产的风险来源，从而精准定位风险发生的可能性与影响程度，最终为企业呈现一幅完整且准确的风险处置菜单；

- **量化分析和评价信息科技风险。**风险处置的前提是理解风险对于公司业务的影响程度，也就是说在处置风险之前必须明确风险一旦发生公司的业务会遭受什么样的损失，以及这种情况发生的概率究竟有多大？这就离不开量化的分析和评价。安言的 ISO/IEC /IEC 31000:2009 风险评估方法科学的利用了模糊理论和概率论方法，将定性的风险评估与定量的方法相结合，最终呈现给客户一套数字化的风险评估结论，支撑客户做出科学的风险处置决策；

- **区分风险优先级，保障处置成本收益最大。**风险处置并非故意而为，而应使处置风险的成本收益与业务发展方向和重要性相符合，利用安言 ISO/IEC /IEC 31000:2009 风险评估方法中的影响范围识别，可以清晰地呈现所识别的风险对于企业业务网络的影响区间和作用深度，从而杜绝了常见风险评估方法仅根据风险的相对高低决定处置的优先级，而忽略了非重要风险往往可能导致关键的业务模块和流程不可用；

- **管理和技术并重，确保措施落地。**信息安全风险管理总离不开信息处理

设施的技术保障措施，单纯使用管理手段无法弥合业务信息系统和技术缺陷间的漏洞，因此安言在其综合风险评估方法中加入了诸多技术评估的环节，如漏洞扫面和渗透测试等，使风险评估的结果也展示了与业务信息系统相关的技术架构的缺陷和薄弱环节，以及由于这些漏洞的存在而可能导致的风险，在互联网安全局势日益严峻的今天这一点显得尤为重要，不仅如此，风险评估的技术环节还能为安全管理措施的落地提供技术层面的参考。



安言咨询信息安全风险管理框架