

PCI DSS v4.0 变更系列之三

——通过“定制方法”增加标准的灵活性

1 通过“定制方法”（customized approach）增加了灵活性

这部分来自于 PCI DSS v4.0 的第八个章节（实施和验证 PCI DSS 的方法），是 PCI DSS v4.0 的一个亮点，也是区别于 v3.2.1 版本的一个巨大的变化。基于此，通过本篇对新出现的“定制方法”进行较详细的说明。

在 v3.2.1 及以前的 PCI DSS 版本中，均使用规定方法（defined approach）所定义的要求作为审核要求，即具体的要求点，提出明确的标准要求及审核方法（参见图 1 右半部分绿色字体的路径）。而对于产业因技术或业务限制无法实施的要求点，PCI DSS 标准允许在特定的前提（存在已知的技术或业务限制、且确保控制的效果不低于标准要求）下，使用补偿性控制措施（Compensating controls）来作为达到合规要求的一种手段（参见图 1 右侧中间的文字描述）。归纳来看，v3.2.1 版本中要么按照达到标准要求点的方式达到合规，要么是在存在技术或业务限制的前提下通过补偿性控制来达到合规要求。

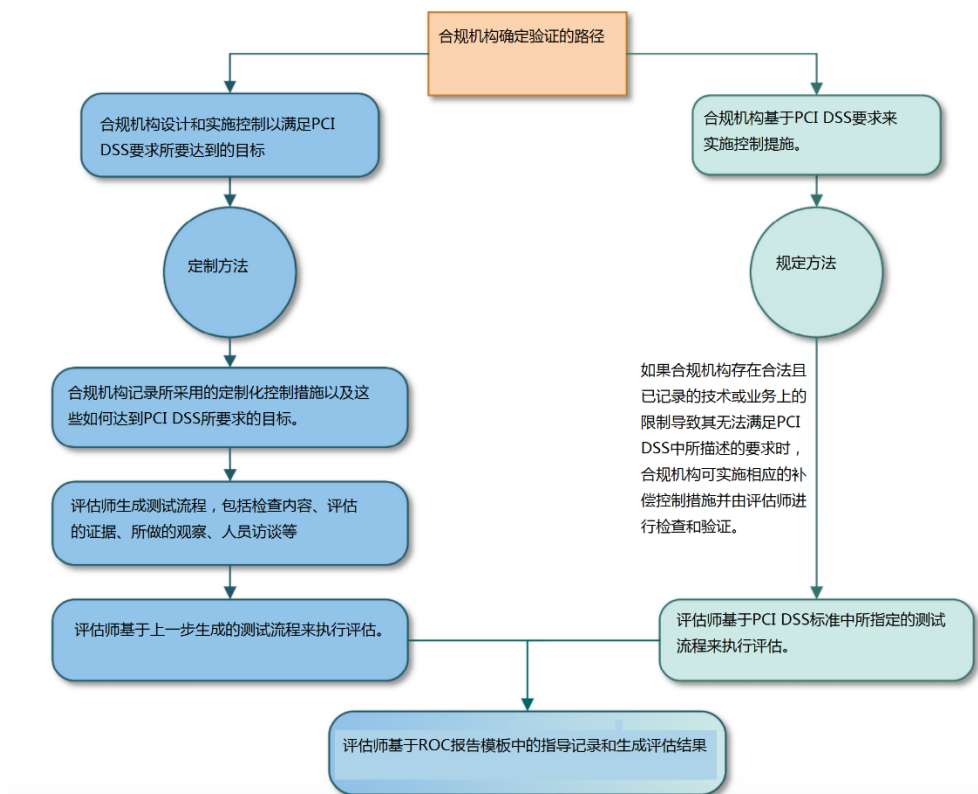


图 1：定制方法与规定方法的审核路径

在 v4.0 中，除了保留规定方法和补偿性控制措施外，还重磅引入了定制方法（customized approach）的合规方式。定制方法本质上是在要求所对应的控制目标不变的前提下，被审核机构针对 PCI DSS 要求及其审核方法进行自行定义和重新编写，可以理解为合规机构基于其技术特点和安全管理能力自行进行对应的标准要求点的编写，并由评估机构对这些自行编写的标准要求点进行验证。

如果采用定制方法，需要合规机构参照 PCI DSS 附录 E 的“E1 控制矩阵模板”记录所制定的控制措施，并参照“E2 风险目标分析模板”进行控制措施的风险分析。审核机构在满足独立性的前提下，由独立的评估师基于措施及风险分析的情况制定测试流程（包括但不限于观察流

程、检查配置、人员访谈、策略与流程检查、检查文档等），并完成相应的验证工作。最后，由评估师在 ROC 合规报告中呈现定制方法的实现、验证情况以及评估结果。

因为定制方法支持安全技术等方面的技术创新和实践，使得合规机构有更多的方式来达到 PCI DSS 要求所对应的目标。定制方法通常适用于信息安全风险管理能力强、技术/安全架构先进的机构。为便于大家理解，我们对规定方法和定制方法的优缺点进行了简单归纳。展示如下表所示：

	规定方法（defined approach）	定制方法（customized approach）
所适用的机构	采用当前主流技术的合规机构。	所采用的技术架构与主流技术差异大，风险管理能力强的机构。
PCI DSS v3.2.1 要求的审核方法的差异	审核方法与原 PCI DSS v3.2.1 相同。	新的达到合规和审核的方式，增加了灵活性，以适用于标准所定义的要求与合规机构的实现机制存在差异的情况。
对合规和审核工作量的影响	无大的影响，工作量与原 PCI DSS v3.2.1 基本一致。	有工作量的影响。主要体现在： 1）合规机构需要制定额外的控制措施，并对剩余的安全风险进行记录和分析。 2）审核机构开发相应的审核要求，并完成审核验证。
是否允许补偿控制措施（CCW）	规定方法中允许存在业务或技术限制的前提下制定补偿控制措施。	定制方法中不再允许在此基础上开发补偿控制措施。

表 1：规定方法与定制方法的对比

v4.0 版本在满足标准要求方面比 v3.2.1 更具灵活性。具体体现在：1）站在所有的合规要求点的角度，某些要求点可以选择使用规定方法达到合规要求，而另外一些要求点可以使用定制方法达到合规要求；2）站在某个具体要求点的角度，合规的机构可以二选一，即可以通过规定方法对应的要求来达到合规，也可以使用定制方法来达到合规要求；3）站在同一个要求点的角度，也允许存在同时结合使用两种方法的可能性。比如，该要求点中所覆盖的范围内的一部分被审核的对象用规定方法来达到合规要求，范围内的另一部分被审核对象使用定制方法来达到合规。

在 v4.0 标准文档“PCI 数据安全标准要求与测试程序”中对每一个要求点的具体描述中，既给出了规定方法的要求，同时也给出了定制方法的对应目标（详见“PCI 数据安全标准要求与测试程序”每个要求点所对应的“定制方法目标”）。值得注意，在标准原文中有些要求点是没有定制方法目标的情况下（比如要求 3.3.1-3.3.2），说明这个要求点是不允许使用定制方法达到合规的。

在更适合使用定制方法来达到合规要求的情况下，**atsec** 作为审核机构，会与合规机构一起基于机构自身的技术特点及风险管理能力，定制恰当的技术要求与审核方法，评估技术要求与审核方法的充分性并进行审核，以验证合规机构的合规状态。

对于期望通过定制方法进行审核的机构，也欢迎在第一时间与 **atsec** 咨询团队进行沟通，以确保制定合理的控制措施、进行充分的风险分析。**atsec** 评估师也会在满足独立性要求的前提下，尽早展开定制方法有效性的分析，制定合理的审核方法，并最终完成定制方法及其措施的验证工作。