补充信息

PCI DSS v4.x：关于补偿控制措施和定制方法的指南

版本：1.0

日期：2026 年 6 月

作者：PCI Security Standards Council

文档变更

日期	版本	描述
2026 年 6 月	1.0	初始版本

确认通知：在所有使用目的和情况下，PCI SSC 网站上的英文文本应作为此文件的官方版本。当翻译文本和英文文本之间出现任何歧义和不一致之处时，正确的内容应以该位置的英文文本为准。

目录

文档变更 i
概述 1
受众与目的 1
实施和认证 PCI DSS v4.x 控制措施的选项 2
用例对比：**补偿**控制措施及定制方法的示例 4
补偿控制措施的作用及定制方法 5
实体的角色：补偿控制措施 5
评估商的角色：补偿控制措施 5
实体的角色：定制方法 7
评估商的角色：定制方法 7
补偿控制措施及定制方法的**记录** 10
评估商的独立性 11
参考文献和**辅**助材料 12
附**录**：已完成的**补偿**控制措施和定制方法模板示例 13
实体完成示例：标标性控制工作表 13
实体完成示例：针对定制方法的控制措施矩阵 16
实体完成示例：针对定制方法的目标风险分析 19
供评估商参考的已完成示例：遵从性报告——附录 E 定制方法模板 22

概述

Payment Card Industry Data Security Standard (PCI DSS) 支持以灵活的方式实现安全目标。PCI DSS v4.x 包含两种实施和认证 PCI DSS 控制措施的方法：定义方法和定制方法。这两种方法在目的、要素、文档和认证方面存在差异。

本文重点介绍了每种方法，并：

- 探讨受评估实体的作用
- 阐述了关联评估商的作用，并
- 提供了这些方法的文档以及常见问题的解答。

对于受评估实体，本文档包含以下已完成的示例：

- 标标性控制工作表，
- 一种针对定制方法的控制措施矩阵，以及
- 一种针对定制方法的目标风险分析。

对于评估商而言，本文件包含一份已填写的《遵从性报告——附录 E 定制方法模板》示例。

受众与目的

本文件适用于所有开发、运营、管理或评估补偿控制措施或定制方法的实体。这包括进行 PCI DSS 评估的评估商以及接受评估的实体。

本文档旨在提供实用指南，以支持补偿控制措施和定制方法的一致使用。

PCI Security Standards Council (PCI SSC) 不负责强制执行遵从性，也不负责确定某项具体实施是否符合合规要求。实体应与管理其遵从性计划的组织（如收单机构（商户银行）、支付品牌或其他实体）合作，以了解该实体的遵从性认证和报告责任。

本文件中的指导原则不对 PCI DSS 或任何其他 PCI SSC 标准中的要求进行补充、扩展、替换或取代。本文件发布时，PCI DSS 的当前版本为 v4.0.1；然而，此处提供的通用原则和实践也可能适用于未来版本。

实施和认证 PCI DSS v4.x 控制措施的选项

PCI DSS v4.x 为实体提供了两种实施和认证 PCI DSS 要求的方法——定义方法和定制方法。

“定义方法”是实施和认证 PCI DSS 控制措施的传统方法，自 PCI DSS 第一版起便一直沿用至今。对于因存在合理且有据可查的技术或业务限制而无法满足“定义方法”中所述要求的实体，**补偿控制措施是“定义方法”中的一种选项**。在存在无法更新以满足要求的遗留系统或流程的情况下，通常会使用补偿控制措施。

定制方法侧重于每项 PCI DSS 要求（如适用）的安全目标，允许实体以不严格遵循既定要求的方式实施控制措施，以满足该要求中规定的“定制方法目标”。由于每种定制实施方式各不相同，因此没有既定的测试程序；相反，评估商必须根据具体的实施情况制定适当的测试程序，以便认证所实施的控制措施是否符合既定目标。

定制方法是否适用于所有 PCI DSS 要求？

大多数 PCI DSS 要求均可通过采用既定方法或定制方法来满足。然而，部分要求未明确列出“定制方法目标”，因此无法选择定制方法。

定制方法适用于哪种类型的实体？

定制方法旨在支持安全实践的创新，使各实体能够更灵活地证明其安全控制措施如何满足 PCI DSS 的目标。建议风险管理成熟且在安全方面采取了健全风险管理方法的实体采用此方法，包括但不限于设有专门的风险管理部门或采用全机构范围的风险管理方法。

使用定制方法实施和认证的控制措施，预计将达到或超过定义方法中要求所提供的安全性。因此，验证自定实施方案所需的记录文件和投入精力，也将比采用定义方法时来得更多。

填写 SAQ 的实体可以使用定制方法吗？

自我评估调查问卷（SAQ）不支持定制方法的使用。希望采用定制方法进行认证的实体，可使用 PCI DSS《遵从性报告》（ROC）模板来记录评估结果。关于使用定制方法的疑问，包括符合 SAQ 资格的实体是否可以填写 ROC 来采用定制方法，应始终咨询负责管理遵从性计划的组织，例如支付品牌和收单机构。

补偿控制措施与定制方法有何区别？

需要注意的是，补偿控制措施与定制方法的目的不同。与补偿控制措施不同，补偿控制措施是在组织存在限制且**无法**满足规定要求时使用的，而定制方法则是针对那些**选择**以不同于规定的方式**满足**要求的实体。在这种情况下，该实体必须满足规定的“定制方法目标”，而不是规定的要求。当实体拥有健全的安全流程和强大的风险管理实践，并具备有效设计满足该目标的安全控制的文档记录、测试和维护的能力时，定制方法最为成功。

请注意，即使某实体未针对该要求采用定制方法，仍可审查该要求的“定制方法目标”，以理解该要求的意图。

补偿控制措施与定制方法能否用于同一项要求？

可以。一个实体可以对某些系统组件使用补偿控制措施，并对其他系统组件采用定制方法来满足同一要求。以要求 5.3.1 为例，如果存在合理且有据可查的业务限制，导致某类服务器无法满足该要求，则该实体可针对该类服务器采用补偿控制措施来满足该要求。该实体还可以选择采用定制方法来满足其他系统组件的同一要求，前提是该实体已实施了一种独特的方法来检测和应对最新的恶意软件威胁。该实体还可以使用所述的定义方法，以满足另一组系统组件的相同要求。

如果一个实体设计了一种不符合定制方法目标的定制方法，该实体能否改用补偿控制措施来满足定制方法的目标？

不可以。在采用定制方法的情况下，补偿控制措施并非可选方案。定制方法适用于选择自行制定符合该要求“定制方法目标”的控制措施的组织。如果某组织制定了定制方法，但随后因技术或业务限制而无法满足“定制方法目标”，这意味着该组织设计了一种其自身无法满足的定制方法。这就是为什么补偿控制措施在定制方法中不可行。

如果某实体确定无法通过定制方法满足 PCI DSS 要求，并且存在技术或业务限制，使其无法按照规定满足“定义方法”的要求，则该实体可以选择根据原始的“定义方法”要求实施补偿控制措施。

用例对比：补偿控制措施及定制方法的示例

提供这些示例仅是为了区分可能考虑采用补偿控制措施或定制方法的使用场景。这些用例并非旨在说明适合或推荐在任何特定环境中使用的实际实施或控制措施。该实体应始终与其评估商以及其将向其提交遵从性文件的实体确认任何补偿控制措施或定制控制的可接受性和使用情况。

通过补偿控制措施予以解决	通过定制方法予以解决
要求 3.3.1.2 由于实体不具备禁止存储的技术，因此 SAD 在授权后被存储。	*此要求不符合定制方法的条件。*
要求 3.5.1 由于技术限制，PAN 无法进行加密或以其他方式使其不可读。	
要求 5.2.1 由于技术限制，某些系统无法部署反恶意软件解决方案。	**要求 5.2.1** 已建立机制，可检测所有恶意软件，并阻止其安装或执行。
要求 8.3.6 云服务提供商的工具不允许更改密码配置，且提供的配置不符合 PCI DSS 要求。 *这可以通过补偿控制措施或定制方法来解决，具体取决于所实施的控制措施。*	
	要求 11.3.1 通过内部漏洞扫描以外的方法识别内部漏洞。
要求 11.3.2 由于 ASV 工具即将进行更改，下一次外部漏洞扫描无法按时进行。	*此要求不符合定制方法的条件。*
	要求 11.5.1 使用 IDS/IPS 以外的机制来检测异常网络流量。

补偿控制措施的作用及定制方法

实体的角色：补偿控制措施

实体应在使用补偿控制措施时对其进行定义，并通过填写一份或多份《标标性控制工作表》（CCW）来记录这些补偿控制措施。该实体的 CCW 应包括：

- 明确定义的技术和/或业务限制，这些限制导致该实体无法满足所述的 PCI DSS 要求。
- 补偿控制措施的定义，以及该控制措施如何满足原始要求的目标并应对任何增加的风险的说明：例如，就构成该控制措施的人员、流程、政策和/或技术而言。
- 原始控制措施的目标：
  - 该实体可以使用（但并非必须使用）该要求中的“定制方法目标”作为此目标。
- 补偿控制措施所实现的目标：
  - 这可以是（但并非必须是）针对 PCI DSS 要求的既定“定制方法目标”。
- 对因缺乏原始控制措施而产生的任何额外风险的描述。文档应体现对该风险的理解以及应对措施。
- 说明该实体如何对补偿控制措施的认证和测试方法。
- 对实体为维持补偿控制措施而实施的流程和控制的定义。

PCI DSS v4.x *附录 C* 中包含了一份 CCW 示例：标标性控制工作表。PCI SSC 网站“文档库”中的 PCI DSS 部分提供了*“额外标标性控制工作表”*的模板。

评估商的角色：补偿控制措施

评估商必须在每次年度 PCI DSS 评估期间，对该实体的标标性控制工作表（CCW）进行彻底评估，以确认该（些）CCW 清晰且有效地记录并处理了*附录 C 中的*各项内容：标标性控制工作表，如上文“实体的职责”部分所述。

对于实体记录在案的合理技术或业务限制，评估商无需确认该业务或技术限制是否有效，只需确认该限制已由实体进行了详尽记录。但是，评估商应测试该实体实施的控制要素，以确认补偿控制措施已落实且运行有效。

评估商应：

- 在《遵从性报告》（ROC）或《自我评估调查问卷》（SAQ）中（视情况而定）中纳入该实体的 CCW。
- 对补偿控制措施进行测试，包括检查配置设置、审查文档、观察流程等，具体视所审查的相关要求和控制措施而定。
  - 该要求的测试程序可被视为针对该特定要求所预期开展之测试类型的指南。
- 在填写 ROC 时，对于通过补偿控制措施满足的每项 PCI DSS 要求：
  - 请勾选“补偿控制措施”复选框。

– 请说明评估商的测试和证据如何证明该要求已落实。
– 在评估商的工作底稿中记录所进行的测试，并将相关证据与其他评估证据一并存档。

能否使用补偿控制措施来解决过去未满足的要求？

不可以。对于 PCI DSS v4.x，附录 B：“补偿控制措施”部分已更新，以明确*补偿控制措施不能用于追溯性地解决过去未满足的要求*。允许以这种方式使用补偿控制措施绝非本指南的初衷。例如，本应执行的任务未被执行，而当时也没有采取任何措施来解决这个问题。但是，实体可以实施补偿控制措施，以应对可能影响该任务未来执行效果的诸多因素（例如，预测计划内的系统停机或人员休假）。

补偿控制措施能否用于满足多项 PCI DSS 要求？

可以。可设计补偿控制措施，以缓解因未满足多项要求而带来的风险。但是，该补偿控制措施如何满足各项要求，必须在单独的“标标性控制工作表”中分别予以记录。

必须处理与每项要求相关的所有目标和风险，并且必须针对每项要求独立认证补偿控制措施。

补偿控制措施是否仅需在有限的时间内使用？

不。并没有规定补偿控制措施只能在有限期间内实施；但是，受评估实体应每年审查其补偿控制措施，以确认这些控制仍然有效且必要。例如，新技术或新系统可能需要修订补偿控制措施以满足该要求的目标，或者可能已使补偿控制措施不再必要，从而能够按原规定满足原始的 PCI DSS 要求。

同样，评估商应每年审查该实体的补偿控制措施，以确认它们对于应对风险和满足要求仍然适当且必要。

实体的角色：定制方法

受评估实体负责设计、开发、分析、实施和维护其定制控制措施，包括以下步骤：

- 审查 本文件中"参考文献和辅助材料"部分所列的定制方法信息。
- 定义并记录每个定制控制措施，包括说明该控制措施如何满足该要求的目标。请参考《控制矩阵模板样本》[1]，该模板可用于记录有关定制控制措施的信息。
- 执行 并记录一项目标风险分析，以证明该定制控制措施足够稳健，能够提供至少与"定义要求"等效的保护。请参阅《*目标风险分析模板示例*》[1]，以获取可用于记录定制控制措施相关信息的模板。
- 执行并记录测试，以确认每项定制控制措施都能有效满足该要求的目标。请参考《控制矩阵模板样本》，记录已执行的测试及其结果。
- 描述如何随时间推移对每项控制措施的有效性进行监控和维护。
- 请尽早与评估商沟通，商讨实施定制方法的计划。
- 向评估商提供关于每项定制控制措施的记录文件。

为了使受评估实体能够有效实施和维护其定制控制措施，该实体必须将定制控制措施的责任内化，并主动承担起责任。

评估商的角色：定制方法

采用定制方法时，评估商应提前收到该实体的定制方法文件，以协助评估商执行以下步骤：

- 确认该 PCI DSS 要求符合采用定制方法的条件。
- 审查该实体的文档，以全面了解定制控制措施。
  - 确认已完成并提供了《控制措施矩阵》和《目标风险分析》。
- 确认每项定制控制措施均有充分的文档记录，包括：
  - 文档包含《定制方法控制措施矩阵》和《目标风险分析》模板中规定的所有必要信息。
  - 该文档描述了该定制控制措施如何提供至少与"定义要求"同等的保护水平。
- 审查该实体对定制控制措施所进行的测试及其测试结果，以确定该实体的测试是否足以对控制措施进行全面评估。
- 制定稳健的测试程序，以确保对每一项定制控制措施进行彻底测试。
  - 该实体提供的文档必须足够详细，以便评估商能够理解控制措施的运作方式并制定适当的测试程序。
  - 如果评估商确定该实体的测试对控制措施进行了全面评估，则评估商可选择利用该实体的测试结果，对控制措施的有效性进行自身测试。在这种情况下，评估商应使用与该实体所用不同的样本集。

[1] "示例模板"中包含两个模板：定制方法——1) "定制方法——控制矩阵模板样本"和 2) "定制方法——目标风险分析模板样本 "。该文档可在 PCI SSC 网站的"文档库"中"PCI DSS"栏目下查阅。虽然实体无需遵循这些模板中的具体格式，但根据 PCI DSS 要求 12.3.2 的规定，实体的"定制方法控制措施矩阵"和"目标风险分析"必须包含这些模板中的所有信息。

- 对每项定制控制措施的实施情况进行独立测试。不要仅依赖于该实体的测试结果。评估商进行测试的目的是确定该控制措施是否：
  - 是否符合该要求中的“定制方法”目标，
  - 为确保持续有效性而予以维护，且
  - 足以得出“已落实”的结论。
- 在《遵从性报告》（ROC）中记录每一项定制控制措施，既要在-相关要求部分，也要在 ROC *附录 E 中*记录*：定制方法模板*。
  - 在评估过程中，评估商应针对每个使用定制控制措施以满足 PCI DSS 要求的实例填写本附录。
  - 除了纳入来自实体文档中的关于定制控制措施的信息外，还应包含评估商自行制定的测试程序的详细信息、评估商为确认该控制措施已建立且有效运行而审查的证据，以及评估商所执行的测试结果。

对于定制方法，实体自行执行的测试能否替代评估商的测试？

不可以。实体进行的测试是其实施和维护定制方法的必要组成部分，旨在证明控制措施的有效性，但不能替代评估商进行的测试。评估商必须进行独立测试，并根据该测试的结果得出评估认证结论。如果评估商确定该实体的测试对控制措施进行了全面评估，则评估商可以使用相同的测试，但样本集应与该实体使用的不同。

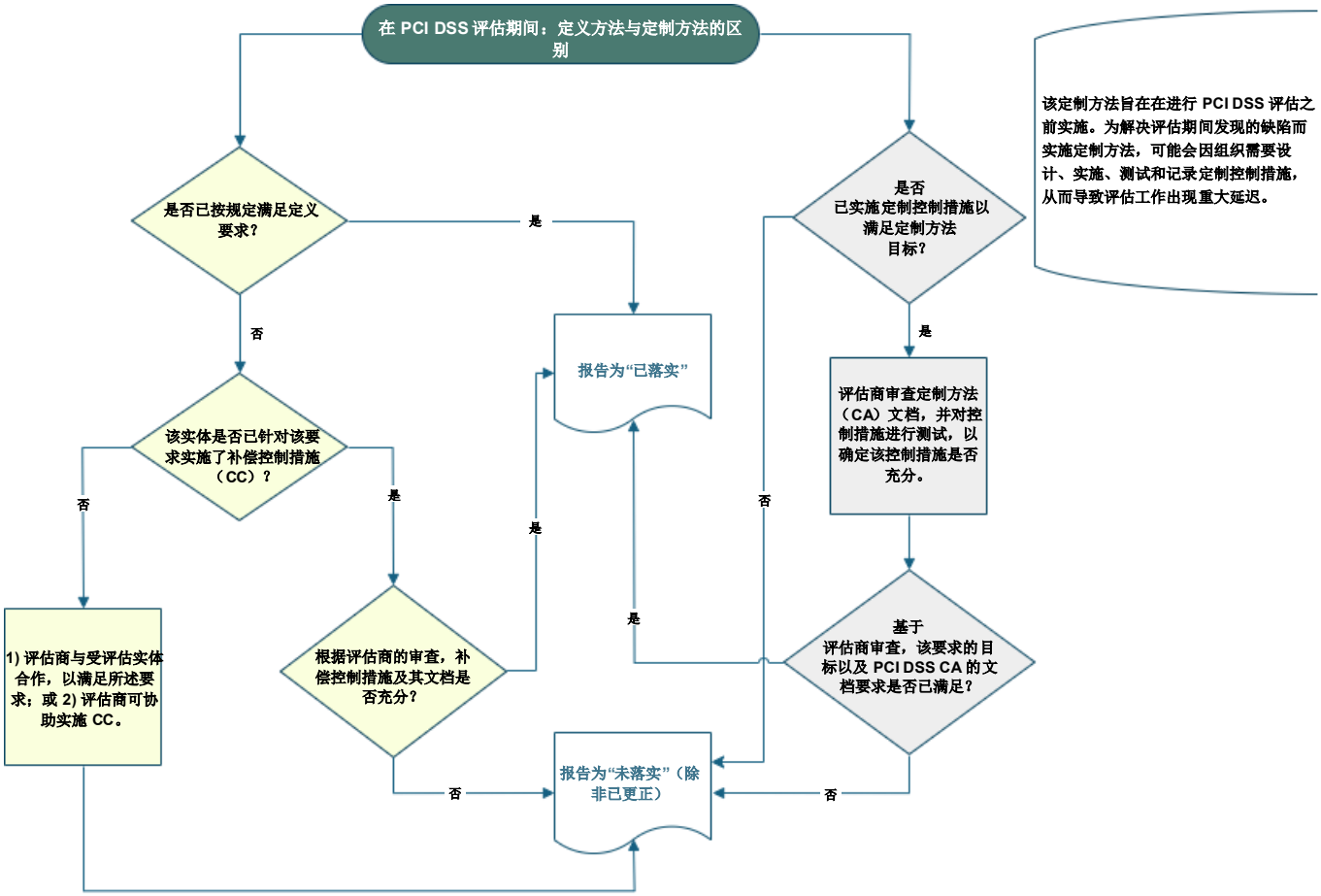
为什么定制方法所需的文档比补偿控制措施更多？

定制实施方案因设计和环境而异，完全由受评估实体自行设计。由于该控制措施由实体自行设计，因此 PCI DSS 中未对其进行定义，也没有预定义的测试程序。因此，实体的文档必须详尽——必须定义该控制措施是什么、如何实施、存在哪些风险、如何应对这些风险、实体如何测试该控制措施、该控制措施如何满足既定目标、实体如何确信该控制措施持续有效等。

该文档使评估商能够全面了解该控制措施及其运作方式，从而制定适当的测试程序并独立认证该控制措施。

下图说明了在 PCI DSS 评估期间，补偿控制措施方法与定制方法之间的区别。

图 1：在 PCI DSS 评估期间，“定义方法”与“定制方法”的区别



补偿控制措施及定制方法的记录

鼓励各实体为其补偿或定制控制措施编制清晰、完整且结构合理的文档。详尽的文档记录为评估商提供了坚实的基础，以便理解和评估控制措施、环境，以及该控制措施如何满足 PCI DSS 要求或目标的意图。

实体的文档质量直接影响评估商认证控制措施并得出有说服力的结论的能力。

无论是补偿控制措施还是定制实施方案，该实体的文档均应：

- 完整、清晰，且独立读者能够理解。
- 能够独立存在，无需依赖未记录的背景信息。
- 清晰地 说明如何实现目标并应对风险。
- 提供证据，说明该实体如何确认控制措施有效运行，包括该实体在认证、测试和持续保证方面的流程及结果的详细信息。

如果实体的文档或证据不完整，是否可以对补偿控制措施或定制方法进行认证？

不可以。如果记录文件不充分，评估商可能无法认证该控制措施的设计和运行是否有效。如果实体未向评估商提供充分证据，或者评估商无法确信实体的文档记录和控制措施是充分的，评估商可以决定是否将“未落实”作为适当的评估结果。

评估商的独立性

评估商的独立性是 PCI DSS 评估的基本原则，在认证补偿控制措施和定制实施方案时同样适用。受评估实体负责补偿控制措施的制定、实施和维护。

QSA 能否代表组织设计或实施控制措施？

虽然 QSA 员工可以协助实体设计或实施控制措施，但 QSA 公司必须遵守 *《QSA 资格要求》* 和 *《QSA 计划指南》* 中规定的独立性要求。这包括实施职责分离控制措施，以确保进行或协助进行 PCI DSS 评估的 QSA 员工保持独立，且不存在任何利益冲突。

如果 QSA 员工曾参与某项控制措施的设计或实施，随后又对补偿或定制性控制措施进行测试、评估或协助评估，则构成利益冲突。有关详细信息，请参阅 PCI SSC 常见问题解答页面上的 *常见问题解答 1562*,“为客户设计、开发或实施特定控制措施的 QSA 员工是否也被允许评估这些相同的控制措施？”。

专门针对定制方法

虽然 QSA 员工可以提供与定制方法相关的咨询服务，但需要 QSA 来设计或实施其定制控制措施的组织可能并不适合采用定制方法，因为该组织可能难以维护该控制措施并确保其持续有效运行。具备风险成熟度、承诺以及开发、实施和维护自身定制控制措施所需资源的组织，更有可能通过定制控制措施实现长期的安全有效性。

评估商或 QSA 公司参与制定补偿或定制控制措施的任何情况，都必须在《遵从性报告》（ROC）的 1.4 节中记录。

参考文献和辅助材料

请参考以下 PCI DSS v4.x 章节和附录，以及以下指导文件、模板和表格：

针对定制方法

- PCI DSS v4.x 简介 第 8 节对比了补偿控制措施与定制方法，并概述了这两种方法。
- PCI DSS v4.x 附录 D 提供了有关定制方法的更多详细信息，包括所需的目标风险分析要素以及实体和评估商的职责。
- 在 PCI DSS v4.x *中，图 5"理解要求各部分"*指明了每个要求中"定义方法要求"的位置，并在适用情况下指明了"定制方法目标"的位置。
- 要求 12.3.2 针对采用定制方法满足的任何 PCI DSS 要求，规定了针对该定制方法的目标风险分析（TRA）的要素。
- PCI DSS 4.x 遵从性报告模板，附录 E 定制方法模板。
- *示例模板："定制方法"*可在 PCI SSC 网站的"文档库"中，PCI DSS 栏目下查阅。本文档包含：
  - 定制方法——控制矩阵模板样本
  - 定制方法——目标风险分析模板样本。
- *PCI DSS v4.x：目标风险分析*指南——描述了 PCI DSS v4.x 中包含的两种不同类型的目标风险分析（TRA）。

关于补偿控制措施

- 在 PCI DSS v4.x 范围内：
  - 第 8 节"引言"，该节对比了补偿控制措施与定制方法，并概述了这两种方法。
  - *附录 B：《补偿控制措施》*，其中提供了定义和基本标准。
  - *附录 C：*标标性控制工作表，这是实体在用于满足 PCI DSS 要求时，用于定义补偿控制措施的工作表示例。
- *额外标标性控制工作表*（供实体记录补偿控制措施使用）可在 PCI SSC 网站的"文档库"中"PCI DSS"栏目下查阅。

附录：已完成的补偿控制措施和定制方法模板示例

实体完成示例：标标性控制工作表

请注意，此内容仅作为填写"标标性控制工作表"的一种示例，并非旨在作为适用于或推荐用于任何特定环境的实际控制措施示例。

要求编号及定义： PCI DSS 要求 8.4.2 – 针对所有进入持卡人数据环境 (CDE) 的访问，均已实施多因素认证 (MFA)。

	所需信息	说明
1. 约束条件	记录导致无法满足原始要求的合理技术或业务限制。	ABC 组织运营着一个旧版支付授权平台（系统 ID：PCIPAY-AUTH-01），该平台运行在专有 UNIX 5.2 版本上。该平台不支持与现代 MFA 机制的集成，包括基于 RADIUS、SAML 或 PAM 的 MFA 模块。该平台由供应商提供支持，但若进行修改，将导致供应商支持失效并损害系统完整性。 根据 PCIPAY-MODERN-02 项目计划，将对该系统进行更换，预计于 2027 年第四季度完成。
2. 补偿控制措施的定义	定义补偿控制措施：说明它们如何实现原始控制措施的目标，以及如何应对增加的风险（如有）。	ABC 组织已实施以下补偿控制措施： **跳板机 MFA 强制执行** 对 PAY-AUTH-01 的所有访问均仅限于位于 VLAN-SEC-ADM 网络段内的专用管理跳板机 。 访问跳板机需要： ▪ 唯一用户 ID ▪ 密码验证 ▪ 基于硬件的验证令牌（经 FIPS 认证的设备） ▪ Active Directory 验证集成 **网络访问控制** 防火墙规则严格限制仅允许通过跳板机访问 PAY-AUTH-01。从用户工作站、VPN 连接或其他网络段直接访问，在技术上已被完全阻断。防火墙规则集参考：FW-RULE-SET-CDE-ADM-V3. **会话监控和日志记录** 所有管理会话均为： ▪ 已集中记录 ▪ 转发至企业 SIEM 平台（SecurityLog-SIEM-01） ▪ 至少保留 12 个月

	所需信息	说明
		会话录制 对 PAY-AUTH-01 的管理会话使用特权访问管理 (PAM) 解决方案 PAM-SEC-01 进行录制。会话记录将保留以供取证和监控之用。 **安全监控与告警** SIEM 会针对以下情况生成警报： ▪ 未经授权的访问尝试 ▪ 在规定的管理时间窗口外进行的访问 ▪ 权限提升尝试 警报由 SOC 人员进行审查。
3. 目标	定义原始控制措施的目标。	通过使用多种验证因素，确保访问 CDE 时的强效验证。
	确定补偿控制措施所实现的目标。 ***注**：这可以是（但并非必须是）PCI DSS 中针对此要求所列明的“定制方法目标”。*	该补偿控制措施通过在授予对 PCIPAY-AUTH-01 的访问权限之前强制实施 MFA，并防止直接访问系统，从而实现了该要求的目标。
4. 已识别风险	识别因原始控制措施缺失而带来的任何其他风险。	无法直接在 PCIPAY-AUTH-01 上实施多因素认证（MFA）相关的风险包括： ▪ 验证凭据可能遭受威胁 ▪ 对持卡人数据系统的未经授权访问 已实施的补偿控制措施通过确保以下方面来缓解此风险： ▪ 在访问前强制执行多因素验证 ▪ 阻止直接访问 ▪ 所有访问均受到监控、记录和审查 残余风险评估为“低”。

	所需信息	说明
5. 补偿控制措施的认证	说明补偿控制措施的认证和测试方式。	该实体通过以下方式认证补偿控制措施的有效性： ▪ 每季度审查防火墙规则（证据：防火墙审查记录)) ▪ 季度特权访问审查（证据：访问审查记录) ▪ 对跳板机上 MFA 执行情况的季度核查 ▪ SIEM 警报月度审查核查 ▪ 特权访问控制年度内部审计 该实体审查了此认证证据，以确认该控制措施有效： ▪ 防火墙配置 ▪ 访问控制配置 ▪ SIEM 警报报告 ▪ 会话录制日志
6. 维护	定义用于维护补偿控制措施的流程和已实施的控制措施。	该实体通过以下方式维持补偿控制措施的有效性： ▪ 规范防火墙和跳板机配置变更的变更管理程序 ▪ 持续的 SIEM 监控 ▪ 季度访问审查 ▪ 补偿控制措施适用性年度审查 补偿控制措施审查负责人：首席信息安全官 审查频率：年度

实体完成示例：针对定制方法的控制措施矩阵

注 此内容仅作为针对定制方法填写控制措施矩阵的一种示例，并非旨在作为适用于或推荐在任何特定环境中使用的实际控制措施的示例。

控制措施矩阵 定制方法模板——已填写示例 由受评估实体填写		
定制控制措施名称/标识符	语音识别与认证	
本控制措施满足的 PCI DSS 要求编号及目标	要求编号：8.2.8	目标：用户会话仅限授权用户使用。
控制措施详情		
已实施的控制措施**有哪些**？	该实体为确保运营规范，运营着一个“零接触”环境。在特定环境下，用户无需使用键盘登录，只需向计算机发出语音命令即可。 用户首次登录系统时，会发出“识别用户名”的语音命令，例如“识别爱丽丝”。 系统首先通过用户的独特声纹对其进行识别和认证，同时调用物理门禁控制系统，以认证用户是否实际位于该环境中。然后，系统会要求用户（例如爱丽丝）复述屏幕上显示的三个随机单词，以防止预先录制，并对声纹进行二次核查。至此，用户已登录。 2.系统会持续监听语音命令。只要已登录的用户身处该物理区域内，其会话就处于活动状态；一旦用户使用门禁卡离开该区域，会话即告终止。 每次用户发出命令时，系统都会认证其声纹。如果与已登录用户的声纹不匹配，则该命令将被拒绝并加以记录。日志由 SIEM 处理。	

控制措施矩阵 定制方法模板——已填写示例 由受评估实体填写	
	如果其他用户尝试使用该用户已登录的终端，声纹将不匹配，系统将拒绝该命令。 例如，如果戴夫（他是系统的授权用户，但未登录爱丽丝的终端）或玛丽（一名恶意攻击者）走到爱丽丝的系统前说“打开舱门”，计算机将识别出该命令并非由爱丽丝发出，并回应“很抱歉，我无法执行此操作”，同时还会记录一次未经授权的访问尝试。 系统已禁用 USB 接口和蓝牙功能，因此无法手动绕过语音识别系统。
控制措施在**何处**实施？	第 17 号生产设施。内华达州。
何时执行控制措施？	每次分析语音请求时。
谁对控制措施承担总体责任和问责？	信息安全负责人
谁负责管理、维护和监控这些控制措施？	安全运营注册部门负责新系统用户的入职工作，其中包括对用户进行培训，并采集足够的语音样本以建立可靠的声纹。 该系统的管理和维护已外包给 Acme Voiceprint Security Technologies 公司，该公司根据要求 12.8 进行管理，并向许多领先的金融机构提供该技术，用于欺诈检测和认证，以及在联络中心访问客户信息。
***对于*所采用的*每一项*PCI DSS 要求，该实体应提供以下详细信息：**	
实体应说明已实施的控制措施如何满足 PCI DSS 要求的***目标***。	只有已登录用户才能使用会话，因为每次发出命令时，系统都会对用户进行有效重新认证（通过声纹生物特征）。其他授权用户和未授权用户无法使用该登录会话。
该实体描述了**其执行的**测试及测试结果，以证明该控制措施符合适用要求的目标。	委托 Acme Secure Testing Services 进行了一次安全评估，以认证系统的运行情况，并尝试对用户会话进行未经授权的访问。他们未能做到这一点。 此外，该公司还进行了一次红队演练，但同样未能威胁系统，也未能冒充授权语音用户获得未经授权的访问权限。

控制措施矩阵 定制方法模板——已填写示例 由受评估实体填写	
实体简要描述了**其进行的**单独风险分析的结果，该分析解释了已实施的控制措施，并说明了这些结果如何验证该控制措施提供的保护水平至少等同于适用 PCI DSS 要求中所定义的方法。有关如何记录此风险分析的详细信息，请参阅单独的《目标风险分析模板》。	根据已定义的要求控制措施，已登录的用户可以离开其工作站，而未经授权的威胁行为者在会话超时之前有 15 分钟的时间访问该工作站。采用此控制措施后，当用户身处该环境时，会话始终处于活动状态；且每条命令在执行前，都会认证其声纹是否源自已登录用户。 因此，该系统所应对的风险级别高于已定义的认证控制措施。
实体描述了其为确保控制措施得以维持并持续保证其有效性而实施的措施。*例如，该实体如何监控控制的有效性、如何发现并应对控制失效，以及采取了哪些行动。*	每月，GRC 团队的一名成员将尝试通过在设施内发出语音命令并使用预先录制的语音来接管用户会话。此演练遵循已记录的程序，结果由系统进行音频录制。每次测试结束后，治理、风险与合规负责人都会审查音频记录和流程日志。 已制定可疑事件报告程序。如果用户怀疑系统对未登录的语音作出了响应，则应遵循相关程序。所有用户都已接受过该程序的使用培训，并已完成了一份模拟事件报告。该程序的使用内容已纳入用户的年度安全培训中。迄今为止，尚未收到任何事件报告。

实体完成示例：针对定制方法的目标风险分析

注 ：此内容仅作为针对定制方法填写目标风险分析的一种示例，并非旨在作为适用于或推荐在任何特定环境中使用的实际控制措施的示例。

针对定制方法的目标风险分析——已完成示例 由受评估实体填写	
项目	**详情**
1. 确定要求	
1.1 准确识别 PCI DSS 的要求原文。	8.2.8 如果用户会话空闲超过 15 分钟，则用户必须重新进行验证以重新激活终端或会话。
1.2 识别该 PCI DSS 要求原文所规定的目标。	用户会话仅限授权用户使用。
1.3 描述该要求旨在防范的恶意行为。	内部或外部威胁行为者可能接管合法用户的无人值守会话。威胁行为者将能够执行操作、访问数据并下达命令，而这些行为会被错误地归因于已登录的用户。 可能会发生对系统和数据的未经授权访问。 日志文件将不准确，它记录了已登录用户的身份，但这些操作实际上并非该用户所为。
2. 描述拟议的解决方案	
2.1 定制控制措施名称/标识符	语音识别与认证
2.2 拟议的解决方案将对现有需求文档中的哪些部分进行修改？在拟议的解决方案中，现有要求原文中的哪些部分将会发生变化？	当前使用的系统并未明确区分活动状态和空闲状态，因此无法检测到会话已“空闲” 15 分钟。相反，登录后的用户在通过初始验证并登录后，可以随时向系统发出语音命令；但是，系统会验证每条发出的命令，以确保该命令确实由已登录的用户发出。 系统只接受已登录用户发出的命令。
2.3 拟议的解决方案将如何防止恶意行为？	由于每个语音命令在执行前都会经过验证，因此除已登录用户以外的任何人发出的命令都将无法通过验证，系统也不会执行该命令。因此，这可以防止内部或外部威胁行为者接管合法用户的无人值守会话。

针对定制方法的目标风险分析——已完成示例 由受评估实体填写						
项目	**详情**					
3. 分析导致持卡人数据机密性遭到泄露的恶意行为发生的概率是否发生任何变化						
3.1 描述控制措施矩阵中详细列出的、影响恶意行为发生可能性的因素。	系统接收到的每条命令都会经过认证，以确保其确由已登录用户发出。这降低了已登录的会话被威胁行为者接管的可能性。根据定义的要求，威胁行为者有 15 分钟的时间窗口，可以物理访问一个无人看管的已认证会话并接管该会话。 在已部署的控制措施中，威胁行为者无法在已登录用户的会话下发出命令。					
3.2 描述在应用定制控制措施后，恶意行为仍可能发生的原因。	该系统已经过广泛测试，不会被语音合成和录音播放等技术解决方案所攻破，而且预计即使有人尝试这些手段，已登录的用户也会察觉到，因为用户必须身处该环境中才能保持登录状态。 威胁行为者可以通过对已登录用户进行身体恐吓来绕过该控制措施；但是，该系统配备了一个危急状况监测器，该监测器不会向用户显示任何激活提示，但会向安保人员发出警报。 在安全测试和评估演练中，模拟攻击者未能绕过该系统。					
3.3 与定义的方法要求相比，定制方法中详细说明的控制措施在多大程度上改变了恶意行为发生的概率？	发生恶意行为的可能性较高	☐	无变化	☐	发生恶意行为的可能性较低	☒
3.4 请说明您对定制控制措施落实后，恶意行为发生可能性变化的评估依据。	由于每条命令都会被认证为来自已登录用户，因此威胁行为者接管已登录用户会话所需满足的 15 分钟时间窗口已缩短为零分钟。					
4. 分析未经授权访问帐户数据对影响的任何变化						
4.1 就本解决方案所涵盖的系统组件范围而言，如果该解决方案失效，将有多少帐户数据面临未经授权访问的风险？	**4.1.1** 存储的 PAN 数量	无。该实体不存储 PAN。	**4.1.2** 12 个月内处理或传输的 PAN 数量	3200 万		

针对定制方法的目标风险分析——已完成示例 由受评估实体填写	
项目	**详情**
4.2 说明定制控制措施将如何直接： 在威胁行为者成功威胁的情况下，减少遭受威胁的个人 PAN 数量，和/或 能够更快地向支付卡品牌通报遭受威胁的 PAN。	已部署的控制措施无法减轻未经授权访问帐户数据所造成的影响。
5. 风险审批与审查	
5.1 我已审阅上述风险分析，并同意所详述的拟议定制方法，其提供的保护水平至少等同于适用 PCI DSS 要求中所定义的方法。	[签名]
5.2 必须在以下日期之前对本风险分析进行审查和更新：	[日期]

供评估商参考的已完成示例：遵从性报告——附录 E 定制方法模板

请注意，此内容仅作为填写《遵从性报告》的一种示例，并非旨在作为适用于或推荐在任何特定环境中使用的实际控制措施的示例。

要求编号及定义：PCI DSS 要求 8.2.8：如果用户会话空闲超过 15 分钟，则用户必须重新进行验证以重新激活终端或会话。

遵从性报告 定制方法模板——已完成示例 由评估商填写	
请列出用于实现"定制方法目标"的每个控制措施的**定制控制措施名称/标识符**。 *（**注**：请使用受评估实体控制措施矩阵中的"定制控制措施"名称。）*	语音识别与认证
描述用于实现"定制方法"目标的**各项控制措施**。 *（**注**：请参阅《支付卡行业数据安全标准》（PCI DSS）中关于"定制方法"目标的要求和测试程序。）*	目标：用户会话仅限授权用户使用。 1. 用户仅可通过语音命令登录系统。系统首先通过用户的独特声纹对其进行识别和认证，同时调用物理门禁控制系统，以认证用户是否实际位于该环境中。然后，系统会要求用户复述屏幕上显示的三个随机单词，以防止预先录制，并对声纹进行二次核查。 2. 系统会持续监听语音命令。只要已登录的用户身处该物理区域内，其会话就处于活动状态；一旦用户使用门禁卡离开该区域，会话即告终止。 3. 每次用户发出命令时，系统都会认证其声纹。如果与已登录用户的声纹不匹配，则该命令将被拒绝并加以记录。日志由 SIEM 处理。 4. 如果其他用户尝试使用该用户已登录的终端，声纹将不匹配，系统将拒绝该命令。 5. 系统已禁用 USB 接口和蓝牙功能，因此无法手动绕过语音识别系统。
描述该控制措施**如何**满足"定制方法"的目标。	定制方法目标：用户会话仅限授权用户使用。 只有已登录用户才能使用会话，因为每次发出命令时，系统都会对用户进行有效重新认证（通过声纹生物特征）。其他授权用户和未授权用户无法使用该登录会话。

遵从性报告 定制方法模板——已完成示例 由评估商填写		
确定已审查的**《控制措施矩阵》文档**，该文档支持针对此要求采取定制方法。		Doc-10 – 定制方法控制措施矩阵
确定已审查的、支持该要求定制方法的“**目标风险分析”文档**。		Doc-11 – TRA 的定制方法
请列明证明以下内容的评估商姓名： 该实体已填写控制措施矩阵，其中包含《PCI DSS v4.x》中“控制措施矩阵模板”所规定的所有信息：PCI SSC 网站上支持定制方法的示例模板，且控制措施矩阵的结果支持针对此要求的定制方法。 该实体已完成目标风险分析，包括 PCI DSS v4.x 中“目标风险分析模板”中规定的所有信息：PCI SSC 网站上支持定制方法的示例模板，且风险分析结果支持针对此要求采用定制方法。		约瑟芬·阿塞索
描述评估商为**认证已实施的控制措施是否符合“定制方法”目标而**制定并执行的**测试程序**；例如，定制控制措施是否足够稳健，能够提供至少与定义方法相当的保护水平。 ***注 1***：*应在可能且适当的情况下进行技术审查（例如，审查配置设置、运行有效性等）。* ***注 2***：*根据需要，为每个评估商制定的测试程序添加额外行。确保为每个新增的“评估商制定的测试程序”复制“评估商制定的测试程序”右侧的所有行。*		
请在此处输入评估商制定的测试程序： 1.a) 进入环境后，如有可用键盘，请尝试通过该键盘登录系统。 1.b) 进入环境后，尝试通过所需的语音命令登录系统。	**确定测试内容**（例如，受访人员、审查的系统组件、观察到的流程等） ***注意***：*所有受测项目必须具有唯一标识。*	在内华达州第 17 号生产设施的环境中，在 Int-1、Int-2 和 Int-3 的协助下，在已启用“定制方法控制措施”的 ConsoleA 和 ConsoleB 上执行了测试。 与 Int-10 进行了沟通，以确认在测试 1 和 2 期间记录并审查了异常情况。
	确定针对此测试程序审查**的所有证据**。	已审查文档 Doc-22——测试 1 和 2 期间的 SIEM 日志。

遵从性报告 定制方法模板——已完成示例 由评估商填写		
1.c) 授权用户登录系统后，请复述屏幕上显示的三个随机单词。 1.d) 用户登录系统后，请另一位授权用户复述屏幕上显示的三个随机单词。 2.a) 在授权用户在场的情况下，以评估商的语气发出语音命令。 2.b) 在授权用户使用门禁卡离开该区域后，使用该用户下达命令的语音录音向系统发出语音指令。 3.a) 查看 SIEM 日志，了解测试 1 和测试 2 的结果。 3.b) 与负责审查 SIEM 日志的人员沟通，以确定他们在测试 1 和测试 2 期间是否捕获了任何异常情况。 4.a) 已在 2.b 中测试。 5.a) 检查系统是否具备 USB 接口和蓝牙功能。	**描述**评估商针对此测试程序所进行的测试**结果**，以及这些结果如何验证已实施的控制措施符合“定制方法”的目标。	评估商跟随一名授权用户进入包含 ConsoleA 和 ConsoleB 的环境。 测试 5.a) 首先，评估商检查了控制台，以确认系统的 USB 接口和蓝牙功能不可用。 测试 1.a) 随后，评估商发现两台控制台均无可用键盘可用于登录。 测试 1.b) 随后，评估商尝试通过所需的语音命令登录系统。系统显示一条错误信息，称评估商不是授权用户，无法登录。 测试 1.c) 随后，评估商观察了 Int-1 登录各控制台的过程，并注意到他使用了一条语音命令，该命令被各控制台接受。随后，评估商复述了每个控制台屏幕上显示的三个单词，并注意到系统未登录该用户，且显示了一条错误信息，称无法识别该用户的语音响应。 测试 1.d) 评估商观察到，Int-2 复述了屏幕上显示的三个随机单词。系统拒绝允许 Int-2 访问系统，并发出通知称声纹不匹配。 测试 2.a) 当 Int-1 成功登录系统，且系统似乎响应了 Int-1 打开文件 xyz 的命令后，评估商向系统发出命令，要求打开文件 xyz。系统拒绝打开该文件，并发出警告信息，称声纹与授权用户不符。 测试 2.b 和测试 4.a）评估商观察到，已登录的用户使用其门禁卡离开了环境。在已登录用户离开环境后，评估商尝试使用之前用户向系统发出命令的记录向系统发出命令。系统拒绝执行该命令，并返回响应称用户已从系统注销。 测试 3.a.)评估商获取了测试期间生成的 SIEM 日志，并验证了系统已正确记录了失败的访问和命令尝试。 测试 3.b) 评估商采访了 Int-10，以核实她是否收到了有关尝试访问系统的警报。 评估商确定，该控制措施按设计运行，且设计似乎能够有效地将用户会话限制在仅获得授权访问的用户范围内。

遵从性报告 定制方法模板——已完成示例 由评估商填写		
记录评估商为**认证控制措施是否得到维护以确保其持续有效性而**制定和执行的**测试程序**；例如，该实体如何监控控制措施的有效性，以及如何检测和应对控制失效，并采取相应措施。 ***注 1：****应在可能且适当的情况下进行技术审查（例如，审查配置设置、运行有效性等）。* ***注 2：****根据需要，为每个评估商制定的测试程序添加额外行。确保为每个新增的"评估商制定的测试程序"复制"评估商制定的测试程序"右侧的所有行。*		
请在此处输入评估商制定的测试程序： 1) 审查 GRC 关于每月测试控制措施的书面程序。 2) 审查过去 12 个月内测试结果的日期和时间，以核实测试是否每月进行。 3) 选择两条记录在案的检测结果，以验证控制措施是否按预期发挥作用，以及 GRC 负责人是否已审核了这些结果。 4) 审查已记录的可疑事件报告程序，并核实该程序是否充分描述了在系统对未登录的语音作出响应时，相关人员应采取的具体措施。 5) 审查年度安全培训材料，以确认所有用户都已接受过该程序的使用培训。 6) 随机选取五份模拟事件报告，审查其完整性。 7) 如果发生了经核实的事件，请审查该事件报告。审查所有已核实的事件报告。	**确定测试对象**（例如，受访人员、审查的系统组件、观察到的流程等） ***注****：所有被测试的项目必须具有唯一标识。*	GRC 程序（Doc-3）及过去 12 个月的测试结果（Doc-4）， 已对 Int-1 进行面谈，并审查了 2025 年 3 月和 2025 年 8 月的测试结果（Doc-16、Doc-17） 与 Int-1 一起审查了书面可疑事件报告程序。 与 Int-1、Int-2 和 Int-3 一起审查了年度安全培训材料。审查了由 Int-10 至 Int-14 填写的模拟事件报告。 已核实过去 12 个月内未发生任何事件。
	列出针对此测试程序审查**的所有证据**。	测试 1：Doc-3 测试 2：Doc-4 测试 3：Doc-16、Doc-17、Int-01 测试 4：Doc-20 测试 5：Doc-23 测试 6：Doc-50、51、52、53、54

遵从性报告 定制方法模板——已完成示例 由评估商填写		
	描述评估商针对此测试程序所进行的测试**结果**，以及这些结果如何验证已实施的控制措施是否得到维持，以确保其持续有效。	GRC 每月测试控制措施的程序似乎清晰且有效，能够确定语音命令控制措施是否按预期运行。GRC 每月完成测试，并按照程序所述的方式进行了记录。测试结果似乎已得到充分记录，包括测试时间、测试人员以及测试结果。 可疑事件报告程序似乎清晰且充分。报告要求包括一份表格（事件报告），第 17 号生产设施的 IT 人员必须使用该表格。内华达州。已确认第 17 号生产设施的所有 IT 员工。内华达州已通过审查从人力资源部获取的培训日志完成了培训。此外，从人力资源部记录中随机抽取了五份模拟事件报告，发现它们均按照程序填写。 与 Int-1 一起审查了从 Int-1 处获得的过去 12 个月的事件日志。虽然日志中记录了若干事件，但似乎均与语音命令控制措施无关。已与 Int-1 确认，未发生与该控制措施相关的事件。 因此，该控制措施的维护似乎确保了将用户会话限制在登录系统的授权用户范围内的持续有效性。