

Số: 2340/2024/TB-NHNA-37

TP.HCM, ngày 18 tháng 10 năm 2024

**THƯ MỜI CHÀO GIÁ***Dự án tư vấn và đánh giá cấp chứng chỉ PCI DSS***Kính gửi: QUÝ CÔNG TY**

Ngân hàng TMCP Nam Á (Nam A Bank) có nhu cầu triển khai dự án tư vấn và đánh giá cấp chứng chỉ PCI DSS, hình thức lựa chọn đối tác theo phương thức chào giá cạnh tranh.

Nay Nam A Bank kính mời các Công ty có đủ năng lực, kinh nghiệm và điều kiện tham gia chào giá cạnh tranh theo các nội dung hướng dẫn cụ thể như sau:

**I. Mô tả yêu cầu****1.1 Yêu cầu nội dung công việc**

Giải pháp triển khai dịch vụ tối thiểu bao gồm các nội dung công việc thực hiện theo các giai đoạn sau:

STT	Nội dung dịch vụ	Phạm vi/ Số lượng	Kết quả đầu ra
<b>Giai đoạn 1: Khảo sát, tư vấn xây dựng phạm vi và đánh giá tính đáp ứng</b>			
1.1	Khảo sát hiện trạng theo tiêu chuẩn PCI DSS v4.0	01 lần	
1.2	Tư vấn phạm vi áp dụng tiêu chuẩn PCI DSS v4.0	01 lần	Báo cáo tư vấn phạm vi áp dụng tiêu chuẩn PCI DSS v4.0
1.3	Phân tích GAP và lập kế hoạch khắc phục các điểm chưa tuân thủ theo tiêu chuẩn PCI DSS v4.0 (GAP Analysis)	01 lần	- Báo cáo phân tích GAP - Kế hoạch khắc phục các điểm chưa tuân thủ
<b>Giai đoạn 2: Tư vấn khắc phục các điểm chưa đáp ứng và thực hiện các hoạt động đảm bảo tuân thủ</b>			
2.1	<b>Thực hiện các hoạt động đảm bảo tuân thủ PCI DSS</b>		
1	Rà quét ASV (ASV Scan)	01 lần	Báo cáo ASV Scan



STT	Nội dung dịch vụ	Phạm vi/ Số lượng	Kết quả đầu ra
2	Rà quét điểm yếu bên trong (Internal vulnerability assessment)	01 lần	Báo cáo rà quét điểm yếu từ bên trong
3	Kiểm thử phân tách mạng (Segmentation pentest)	01 lần	Báo cáo kiểm thử chia tách lớp mạng
4	Rà quét dữ liệu thẻ (CDD Scan)	01 lần	Báo cáo rà quét dữ liệu thẻ
5	Đào tạo nhận thức về PCI DSS (Awareness training)	01 lần	- Kế hoạch đào tạo - Tài liệu đào tạo - Báo cáo đào tạo
6	Kiểm thử bảo mật ứng dụng phần mềm (Application pentest)	01 lần	Báo cáo kiểm thử bảo mật ứng dụng
7	Review bộ luật tường lửa (Firewall rule set review)	01 lần	Báo cáo review bộ luật tường lửa
8	Rà quét mạng không dây (Wireless scan)	01 lần	Báo cáo rà quét mạng không dây
9	Kiểm thử bảo mật nội và ngoại mạng (Internal & External network pentest)	01 lần	Báo cáo kiểm thử bảo mật nội mạng Báo cáo kiểm thử bảo mật ngoại mạng
10	Đánh giá rủi ro phạm vi PCI DSS (PCI DSS Risk assessment)	01 lần	Báo cáo đánh giá rủi ro phạm vi PCI DSS
11	Tư vấn xây dựng, sửa đổi các chính sách, quy định, quy trình chưa đáp ứng PCI DSS (Policy review)	01 lần	
<b>2.2</b>	<b><i>Tư vấn khắc phục các điểm GAP tìm thấy trong giai đoạn 1</i></b>		



STT	Nội dung dịch vụ	Phạm vi/ Số lượng	Kết quả đầu ra
1	Tư vấn định kỳ và đột xuất để giám sát tiến độ khắc phục và hướng dẫn cách thức khắc phục các điểm GAP, điểm chưa đáp ứng tuân thủ		- Theo dõi kết quả thực hiện khắc phục GAP - Có phương án điều chỉnh ngay khi có phát sinh
<b>Giai đoạn 3: Đánh giá và cấp chứng chỉ tuân thủ PCI DSS level 1</b>			
<b>3.1 Đánh giá thử (Pre-Audit)</b>			
1	Thực hiện đánh giá thử và khắc phục GAP tìm ra sau đánh giá thử (nếu có)	01 lần	Báo cáo đánh giá thử
<b>3.2 Đánh giá cấp chứng chỉ (Certification Audit)</b>			
1	Đánh giá cấp chứng chỉ: - Đánh giá chính thức của QSA	01 lần	
2	- Soạn thảo bộ tài liệu tuân thủ - Đảm bảo chất lượng báo cáo tuân thủ - Cấp chứng chỉ PCI DSS level 1	01 lần	- Tuyên bố tuân thủ (AOC) - Báo cáo tuân thủ (ROC) - Chứng chỉ tuân thủ PCI DSS level 1

## 1.2 Yêu cầu về thời gian dự kiến triển khai

Tổng thời gian thực hiện dự kiến 12 – 18 tháng, bao gồm các giai đoạn chính như sau:

STT	Công việc	Thời gian
I	Giai đoạn 1: Khảo sát, tư vấn xây dựng phạm vi và đánh giá tính đáp ứng	01 - 03 tháng
II	Giai đoạn 2: Tư vấn khắc phục các điểm chưa đáp ứng và thực hiện các hoạt động đảm bảo tuân thủ	09 - 12 tháng
III	Giai đoạn 3: Đánh giá và cấp chứng chỉ tuân thủ PCI DSS level 1	02 - 03 tháng

## II. Yêu cầu đối với đối tác

Đối tác phải có chứng chỉ QSA (Được ghi nhận tại trang web chính thức của PCI SSC: ([https://listings.pcisecuritystandards.org/assessors\\_and\\_solutions/qualified\\_security\\_assessor](https://listings.pcisecuritystandards.org/assessors_and_solutions/qualified_security_assessors)s) với các yêu cầu về kinh nghiệm và năng lực như sau:

STT	Mô tả về mức yêu cầu tối thiểu
<b>A</b>	<b>Yêu cầu về kinh nghiệm</b>
1	- Có ít nhất 03 hợp đồng Tư vấn và đánh giá chứng chỉ PCI DSS cho các ngân hàng và tổ chức tài chính khác nhau đã thực hiện trong các năm gần đây (2021, 2022, 2023), trị giá mỗi hợp đồng lớn hơn hoặc bằng 1,5 tỷ đồng (kèm bản sao các hợp đồng để chứng minh).
2	Cung cấp đủ số lượng và chất lượng nhân sự đáp ứng yêu cầu của Nam A Bank để triển khai dự án;
3	Cung cấp đầy đủ CV của từng nhân sự tham gia dự án theo đúng yêu cầu tiêu chuẩn của Nam A Bank.
4	Cam kết các nhân sự gửi CV khi tham gia thầu sẽ tham gia dự án toàn thời gian khi triển khai; hoặc có nhân sự thay thế tương đương với các nhân sự này khi có thay đổi trong quá trình triển khai dự án
<b>B</b>	<b>Năng lực sản xuất kinh doanh</b>
5	Có giấy phép kinh doanh sản phẩm, dịch vụ an toàn thông tin mạng được cấp bởi Bộ thông tin truyền thông
6	Được công nhận trên trang web chính thức của PCI SSC dành cho các công ty công nghệ đủ năng lực để cấp chứng chỉ PCI DSS phiên bản mới nhất tính tới thời điểm hiện tại (v4)
7	Có chi nhánh, trung tâm bảo hành, bảo trì, xử lý sự cố tại TPHCM. Nhà thầu phải cung cấp tài liệu chứng minh có chi nhánh, trung tâm bảo hành, bảo trì, xử lý sự cố tại TPHCM. (Giấy phép kinh doanh, v.v..) $\geq$ 01 Trung tâm
<b>C</b>	<b>Năng lực tài chính</b>
8	Vốn điều lệ $\geq$ 02 tỷ đồng



STT	Mô tả về mức yêu cầu tối thiểu
9	Lợi nhuận trong hai (02) năm gần nhất (kèm bản sao báo cáo tài chính chứng minh) > 0
<b>D</b>	<b>Năng lực nhân sự triển khai chủ chốt</b>
10	<p>Giám đốc dự án:</p> <ul style="list-style-type: none"> <li>- Số lượng <math>\geq 01</math></li> <li>- Có ít nhất 10 năm kinh nghiệm trong lĩnh vực tư vấn giải pháp bảo mật</li> <li>- Chứng chỉ: CCIE, CCNP hoặc tương đương.</li> </ul>
11	<p>Chuyên gia tư vấn trưởng:</p> <ul style="list-style-type: none"> <li>- Số lượng <math>\geq 01</math></li> <li>- Có ít nhất 7 năm kinh nghiệm trong lĩnh vực tư vấn, đánh giá tuân thủ các tiêu chuẩn An toàn thông tin quốc tế (PCI DSS, ISO 27001, v.v.)</li> <li>- Chứng chỉ: PCI QSA, CISM, ISO 27001:2022 Lead Auditor</li> </ul>
12	<p>Trưởng nhóm dò quét và kiểm thử bảo mật:</p> <ul style="list-style-type: none"> <li>- Số lượng <math>\geq 01</math></li> <li>- Có ít nhất 5 năm kinh nghiệm trong lĩnh vực dò quét và kiểm thử bảo mật</li> <li>- Chứng chỉ: OSCP, OSWE</li> </ul>
13	<p>Chuyên gia tư vấn giải pháp:</p> <ul style="list-style-type: none"> <li>- Số lượng <math>\geq 01</math></li> <li>- Có ít nhất 10 năm kinh nghiệm trong lĩnh vực An toàn thông tin và tư vấn giải pháp bảo mật</li> <li>- Chứng chỉ: CCSP, CISM</li> </ul>

### III. Một số yêu cầu về Hồ sơ chào giá (HSCG)

- Hồ sơ chào giá phải được đóng gói trong phong bì dán kín, các giấy tờ trong Hồ sơ phải có chữ ký của Người đại diện theo pháp luật và đóng dấu của Công ty. Hồ sơ chào giá bao gồm 01 bản gốc và 02 bản sao;
- Hồ sơ chào giá bao gồm:

- + Hồ sơ năng lực của Nhà cung cấp: Báo cáo tài chính 02 năm gần nhất, Giấy chứng nhận đăng ký kinh doanh, Giấy phép đăng ký mã số thuế, Tờ khai quyết toán thuế thu nhập doanh nghiệp năm gần nhất;
- + Tài liệu chứng minh chất lượng dịch vụ (nếu có);
- + Trình bày lộ trình triển khai chi tiết bằng biểu đồ Gantt.
- + Trình bày chi tiết rõ số lượng ngày công (man-day), số lượng nhân sự từng vị trí trong dự án.
- + Trình bày chi tiết hồ sơ năng lực của thành viên ban triển khai dự án.
- + Bảng chào giá chi tiết.
- Đồng tiền trong hồ sơ chào giá: Bằng đồng Việt Nam, giá chào phải bao gồm tất cả các khoản thuế, phí cần thiết;
- Hồ sơ chào giá phải có hiệu lực tối thiểu 60 ngày;
- Thời hạn bảo hành cho dịch vụ tối thiểu là 12 tháng, tính từ ngày nghiệm thu bàn giao dịch vụ.

#### IV. Thời gian và địa điểm nhận HSCG

- Thời gian gửi Hồ sơ chào giá: Trước 17h00 giờ ngày 25./10/2024.  
Các Hồ sơ gửi sau thời gian nêu trên, Nam A Bank sẽ xem xét chấp nhận hoặc không chấp nhận tùy theo tình hình thực tế và phù hợp với quy định.
- Nơi nhận Hồ sơ: Phòng An ninh thông tin, Nam A Bank tại số 201-203 Cách Mạng Tháng Tám, P.04, Q.3, Tp. Hồ Chí Minh.

Nam A Bank kính mời Quý Công ty quan tâm nộp Hồ sơ chào giá theo thời gian và địa chỉ nêu trên.

*Các vướng mắc trong quá trình lập Hồ sơ chào giá, Quý Công ty vui lòng liên hệ Phòng An ninh thông tin – Ông Nguyễn Anh Dũng (ĐT: 0827 827 777)*

**TU. TỔNG GIÁM ĐỐC**  
**PHÓ TỔNG GIÁM ĐỐC**



Nguyễn Vĩnh Tuyên