Phần 2. YÊU CẦU VỀ KỸ THUẬT

Chương V. YÊU CẦU VỀ KỸ THUẬT

1. Giới thiệu chung về gói thầu:

- Tên gói thầu: Thuê dịch vụ phần mềm trên cloud (SaaS): Phần mềm quản lý thiết bị di động (MDM) cho 11000 thiết bị điện thoại thông minh, máy tính bảng trong 3 năm.
- Địa chỉ thực hiện: Tại Ngân hàng TMCP Công Thương Việt Nam
- Quy mô gói thầu:

STT	Nội dung	Đơn vị tính	Số lượng
1	Dịch vụ phần mềm trên cloud (SaaS): Phần mềm quản lý thiết bị di động (MDM) (license tính trên một thiết bị sử dụng trong một năm)-năm thứ nhất	License/năm	11.000
2	Dịch vụ phần mềm trên cloud (SaaS): Phần mềm quản lý thiết bị di động (MDM) (license tính trên một thiết bị sử dụng trong một năm)-năm thứ hai	License/năm	11.000
3	Dịch vụ phần mềm trên cloud (SaaS): Phần mềm quản lý thiết bị di động (MDM) (license tính trên một thiết bị sử dụng trong một năm)-năm thứ ba	License/năm	11.000
4	Dịch vụ triển khai tích hợp	Gói	1

- Thời gian thực hiện gói thầu: 37 tháng kể từ ngày hợp đồng có hiệu lực.

2. Mục tiêu công việc:

- Việc mua sắm thuê dịch vụ phần mềm trên Cloud (SaaS) quản lý thiết bị di động (MDM) cho 11.000 thiết bị điện thoại thông minh, máy tính bảng (Hệ thống MDM) trong thời gian 03 năm nhằm tiếp tục duy trì việc cung cấp cho Ngân hàng một hệ thống CNTT phục vụ việc quản lý tập trung các hoạt động truy cập, làm việc từ xa linh hoạt mọi lúc, mọi nơi thông qua thiết bị di động, đảm bảo an toàn và tiện lợi. Việc triển khai Hệ thống MDM góp phần giảm thiểu rủi ro an toàn thông tin, rủi ro vận hành phát sinh từ việc gia tăng sử dụng thiết bị di động trong công việc, đáp ứng yêu cầu quản lý rủi ro và tuân thủ các quy định nội bộ cũng như quy định pháp luật hiện hành. Qua đó, hệ thống góp phần nâng cao hiệu quả công việc và năng suất lao động chung của Ngân hàng TMCP Công thương Việt Nam.

3. Yêu cầu kỹ thuật của gói thầu:

Yêu cầu tương đương hoặc cao hơn danh mục dịch vụ chi tiết được trình bày tại các bảng sau:

3.1. Yêu cầu kỹ thuật chi tiết như sau

STT	Nội dung
2.1	***Các yêu cầu chung về dịch vụ điện toán đám mây***
1	Giải pháp cho phép Ngân hàng TMCP Công Thương Việt Nam (NHCT) quản lý được các thiết bị di động (bao gồm điện thoại thông minh, máy tính bảng) được đăng ký sử dụng để xử lý công việc cho NHCT. Các thành phần bao gồm tối thiểu: quản lý thiết bị đăng ký vào hệ thống, thiết lập và quản lý cấu hình bảo vệ thiết bị, quản lý quyền và xác thực đa yếu tố với người sử dụng, quản lý việc cài đặt ứng dụng để sử dụng thiết bị di động làm việc hoặc xử lý dữ liệu nội bộ của NHCT, quản lý và mã hóa dữ liệu, cung cấp và quản lý kênh kết nối mã hóa VPN vào nội bộ NHCT.
2	Hệ thống phải hỗ trợ đa dạng các chủng loại thiết bị và hỗ trợ nhưng không giới hạn đối với các thiết bị có hệ điều hành Android, iOS.
3	Mô hình áp dụng SaaS – cung cấp dạng dịch vụ phần mềm trên điện toán đám mây, trả tiền thuê trọn gói tính theo số thiết bị sử dụng. NHCT chỉ cần thuê bản quyền sử dụng dịch vụ phần mềm trên điện toán đám mây theo số lượng thiết bị sử dụng để sử dụng theo phạm vi yêu cầu. NHCT sẽ không phải trả thêm bất kỳ chi phí hạ tầng hay chi phí phát sinh nào khác để sử dụng cài đặt và sử dụng thiết bị an toàn và quản lý tập trung theo các yêu cầu cụ thể dưới đây.
4	Giải pháp có sẵn thành phần quản lý kết nối VPN và ứng dụng VPN client kèm theo để cho phép thực hiện và quản lý được kết nối có mã hóa (VPN) về mạng nội bộ của Ngân hàng theo từng ứng dụng cụ thể; kết nối VPN có thể được thiết lập cơ chế tự động bật ngay khi ứng dụng được phép kết nối VPN khởi chạy và tự tắt sau một khoảng thời gian ứng dụng không còn kết nối VPN (Per App VPN)
5	Có sẵn các hàm tích hợp (API) và bộ công cụ phát triển (SDK) để NHCT có thể chủ động tích hợp với các hệ thống bảo mật, ứng dụng của mình.
6	Hệ thống có khả năng mở rộng quy mô dễ dàng và nhanh chóng. Ngay khi cần mở rộng, NHCT có thể mua bổ sung thêm license thiết bị mà không phải cài đặt gì trên hệ thống.
7	Có cam kết đảm bảo tính sẵn sàng của dịch vụ trong hàng tháng lên tới 99.9% tổng thời gian trong tháng.
2.2	***Yêu cầu giải pháp bao gồm các cấu phần và các yêu cầu cụ thể sau:***
2.2.1	**Yêu cầu đối với việc quản lý người dùng và xác thực**
1	Hệ thống có thành phần hỗ trợ quản lý, xác thực và phân quyền cho người dùng, nhóm người dùng hệ thống thông qua tài khoản tự tạo trên hệ thống hoặc hệ

STT	Nội dung
	thống Active Directory nội bộ của NHCT hoặc các nền tảng quản lý người dùng (IDP) trong nội bộ hoặc cloud khác theo yêu cầu của NHCT.
2	Hỗ trợ xác thực đa yếu tố với người dùng (bao gồm cả quản trị viên và người sử dụng) thông qua các giao thức xác thực LDAP, SAML, và có thể kết hợp yếu tố thứ hai có sẵn với các giao thức xác thực bằng FIDO2, OTP (qua Authenticator app), DUO security, Okta...
3	Hỗ trợ khả năng thiết lập xác thực đa yếu tố theo người dùng hoặc các biện pháp tương đương (như kiểm tra trước đăng ký serial number của máy) đối với việc: đăng ký thiết bị vào hệ thống và trước khi thiết lập kết nối VPN vào nội bộ của NHCT
2.2.2	**Cấu phần MDM (Mobile Device Management): Quản lý thiết bị**
1	Giải pháp phải hỗ trợ được trên các nền tảng thiết bị tối thiểu như sau: Yêu cầu hỗ trợ đầy đủ các yêu cầu tối thiểu với hệ điều hành Android (từ phiên bản 10 trở lên) và iOS (từ phiên bản 12.0 trở lên).
	Cung cấp chức năng tự quản lý thiết bị (selfservices), cho phép người dùng được cấp quyền có thể thực hiện tự đăng ký và quản lý thiết bị; có hỗ trợ xác thực đăng ký bằng hai yếu tố… hoặc xác thực thiết bị bằng serial number hoặc định danh thiết bị trong quá trình cài đặt và đăng ký thiết bị.
	Cho phép cấu hình cơ chế đăng ký có tự động phát hiện và điền (auto discovery) các thông số đăng ký thiết bị ban đầu, chỉ cần nhập email đầy đủ của người dùng
2	Quản lý được trạng thái, thông số cấu hình phần cứng cũng như các thiết lập trên hệ điều hành của thiết bị di động.
3	Hỗ trợ cả thiết bị của công ty, thiết bị cá nhân với các hồ sơ quản lý có thể được thiết lập khác nhau.
4	Gắn thiết bị được quản lý với người dùng, người dùng có thể phân quyền theo user từ hệ thống AD của NHCT, hoặc local hệ thống MDM tự tạo.
5	Hỗ trợ đăng ký theo nhóm người sử dụng, nhóm thiết bị theo nhóm người dùng trên hệ thống Active directory.
6	Thiết lập cấu hình bảo mật trên hệ điều hành của thiết bị, với nhiều hồ sơ bảo mật khác nhau theo nhóm thiết bị hoặc theo người dùng.
7	Cho phép thực hiện tự đăng ký thiết bị, có xác thực người dùng đăng ký bằng đa yếu tố, hoặc kiểm soát thiết bị đăng ký bằng serial number hoặc định danh thiết bị.
8	Hệ thống cho phép tác động vào các chức năng trên hệ điều hành của thiết bị như sau để thiết lập cấu hình bảo mật: xóa thiết bị từ xa (có chọn lọc), đặt lại mã khóa (passcode) trên thiết bị, khóa và mở khóa hệ điều hành thiết bị từ xa, ...
9	Có khả năng quản lý cập nhật OS cho thiết bị di động

STT	Nội dung
10	Giải pháp cung cấp chức năng tắt các tính năng trên thiết bị phần cứng từ xa, như tắt camera, cấm thẻ nhớ, tắt các truyền tín hiệu không dây như bluetooth trên các thiết bị công ty cung cấp,...
11	Giải pháp cung cấp khả năng cấu hình một số tham số của thiết bị từ xa như cấu hình WIFI, Proxy...
12	Có khả năng phát hiện, áp dụng chính sách riêng hoặc từ chối các thiết bị di động đã bị bẻ khóa với các hệ điều hành (tối thiểu với Android và iOS).
13	Có khả năng bật tắt và quản lý vị trí hiện tại của thiết bị (qua GPS).
15	Có khả năng cài đặt cấu hình, áp đặt chính sách một cách tự động và hàng loạt cho các nhóm thiết bị khác nhau dựa trên các tiêu chí khác nhau.
16	Có khả năng tạo các chính sách bảo vệ cho ứng dụng được chỉ định và có thể áp xuống theo nhóm người dùng cụ thể.
18	Có khả năng tạo ra các thiết bị ở dạng kiosk (thiết bị chỉ cho phép truy cập những gì được cho phép trên màn hình chính, có khả năng tùy chỉnh dễ dàng như thêm logo, hình ảnh phù hợp với yêu cầu marketing, nhận diện hình ảnh doanh nghiệp) đối với các thiết bị doanh nghiệp cấp cho nhân viên (phù hợp cho thiết bị dùng chung).
2.2.3	**Cấu phần MAM (Mobile Application Management): Quản lý ứng dụng trên thiết bị**
1	Quản lý từ xa, tập trung được việc cài đặt hoặc gỡ bỏ các ứng dụng được hoặc không được phép cài đặt trên các thiết bị được quản lý.
2	Hỗ trợ quản lý cài đặt từ xa các ứng dụng với từng nhóm thiết bị theo các nhóm người dùng khác nhau.
3	Hỗ trợ triển khai cài đặt từ xa các ứng dụng có định dạng APK (Android), IPA (iOS), hoặc các ứng dụng khác của doanh nghiệp trên thiết bị di động.
6	Cung cấp các ứng dụng mobile sẵn có của giải pháp (như ứng dụng VPN client, ứng dụng đọc Email theo cơ chế Mobile Active Sync, ứng dụng đọc file .docx, doc, excel, pdf, file ảnh jpg.., ứng dụng duyệt web); Cho phép NHCT toàn quyền quản lý các ứng dụng này, bao gồm cài đặt thiết lập các tính năng và thuộc tính bảo mật, bảo vệ ứng dụng, bảo vệ dữ liệu của NHCT bởi chính ứng dụng, ví dụ như thiết lập passcode, chặn screenshot, chống copy dữ liệu, mã hóa file tải xuống bởi ứng dụng,...
7	Hỗ trợ thiết lập cấu hình cho VPN client của giải pháp VPN các hãng khác (như Checkpoint, F5, Palo Alto,...) mà NHCT có thể sử dụng (nhà thầu liệt kê cụ thể các hãng có thể hỗ trợ)
9	Hỗ trợ tách biệt vùng làm việc (work profile) riêng tách biệt so với vùng dữ liệu cá nhân trên thiết bị (tối thiểu là Android).
10	Cho phép chia sẻ được file giữa thiết bị di động và nội bộ qua ứng dụng riêng
11	Hỗ trợ quản lý kết nối đồng bộ email qua giao thức Email Mobile Active sync

STT	Nội dung
2.2.4	**Công cụ quản trị và hỗ trợ người dùng**
1	Giải pháp quản lý thiết bị di động phải cung cấp một giao diện quản trị duy nhất để giám sát được tất cả các thiết bị đã đăng ký.
2	Có khả năng dễ dàng tìm kiếm thiết bị đơn lẻ hoặc nhóm thiết bị theo dạng lọc tổng hợp nhiều tiêu chí.
3	Cho phép import danh sách thông tin thiết bị vào hệ thống để quản lý trước việc đăng ký và trạng thái cấp phát cho người sử dụng.
4	Cho phép cấu hình thu thập và lưu trữ tập trung log các hoạt động của hệ thống
5	Hỗ trợ cơ chế cảnh báo cho người quản trị khi có thiết bị mới enroll, hoặc phát hiện ra sự kiện thiết bị không đảm bảo tuân thủ, ...
6	Có chức năng tạo báo cáo như: thống kê số lượng thiết bị di động theo hệ điều hành, thống kê theo tổ chức (tối thiểu mức tổ chức), thống kê thiết bị máy di động không tuân thủ, trạng thái kết nối, trạng thái cập nhật thiết bị, thiết bị active/deactive, user sử dụng thiết bị...
7	Hệ thống có khả năng quản lý người quản trị (thêm người quản trị, gán vai trò, thiết lập quyền điều khiển, truy cập), có thể tạo nhiều tài khoản quản trị cùng lúc, hỗ trợ xác thực hai yếu tố với người quản trị.
2.2.5	**Các yêu cầu khả năng tích hợp**
1	Giải pháp phải có khả năng tích hợp với hệ thống Microsoft Active Directory nội bộ hiện có của NHCT để xác thực.
2	Có khả năng tích hợp được các nền tảng Cloud khác, tối thiểu là Microsoft Office 365,... mà vẫn đảm bảo được sự đồng nhất về chính sách bảo vệ kết nối, bảo vệ dữ liệu nội bộ cũng như xác thực người dùng nội bộ, khi Ngân hàng triển khai sử dụng các dịch vụ Cloud này cho người dùng nội bộ.
3	Tích hợp được với hệ thống mail Exchange 2016 và các phiên bản cao hơn để người dùng đồng bộ hóa email, lịch và danh bạ với thiết bị.

3.2. Yêu cầu về dịch vụ triển khai tích hợp

Nhà thầu triển khai tích hợp phần mềm trên cloud (SaaS) quản lý thiết bị di động (MDM) phải đảm bảo tương thích với nền tảng MDM hiện có của Ngân hàng TMCP Công thương Việt Nam;

Mọi công việc, bao gồm cả việc cài đặt đủ thiết bị theo số lượng bản quyền đã mua, phải hoàn thành trong **vòng 1 tháng** kể từ ngày hợp đồng có hiệu lực;

Bản quyền có hiệu lực kể từ ngày nghiệm thu triển khai tích hợp;

3.3. Yêu cầu Hỗ trợ kỹ thuật

Nhà thầu cung cấp dịch vụ Hỗ trợ kỹ thuật chính hãng theo phạm vi và yêu cầu sau:

1	**Thời gian làm việc và địa chỉ thực hiện:**
1.1	- Thời gian cung cấp dịch vụ hỗ trợ kỹ thuật: 03 năm (1095 ngày), kể từ ngày nghiệm thu triển khai tích hợp. - Thời gian thực hiện hỗ trợ kỹ thuật: 24 giờ/ngày, 7 ngày/tuần, 365 ngày/năm

1.2	- Địa điểm thông báo hỗ trợ kỹ thuật: Tại Trung tâm dữ liệu Vân Canh và Hòa Lạc của Ngân hàng TMCP Công thương Việt Nam.
2	**Yêu cầu Hỗ trợ kỹ thuật**
2.1	Cung cấp dịch vụ hỗ trợ kỹ thuật chính hãng với các hình thức như hỗ trợ từ xa thông qua kênh Website hỗ trợ của hãng, web chat, email, hoặc họp trực tuyến.
2.2	Riêng đối với thành phần trung gian được cài đặt trong hạ tầng CNTT nội bộ của NHCT để phục vụ cho việc kết nối từ thiết bị máy tính xách tay vào các hệ thống CNTT nội bộ của VietinBank, nhà thầu phối hợp với NHCT thực hiện: - Điều chỉnh, bổ sung thêm thành phần hoặc máy chủ cho thành phần trung gian này theo yêu cầu của hãng hoặc NHCT yêu cầu thực hiện *(nếu có)*. - Cập nhật lên phiên bản mới với các thành phần cài đặt trong nội bộ. - Xử lý các sự cố hoặc vấn đề phát sinh trong quá trình sử dụng. - Trách nhiệm phối hợp với hãng để phân tích nguyên nhân, tìm biện pháp xử lý đảm bảo khắc phục sự cố trong thời gian quy định.
2.3	Cho phép tối thiểu 4 đầu mối kỹ thuật của NHCT trên hệ thống hỗ trợ chính hãng
2.4	Không giới hạn số yêu cầu hỗ trợ kỹ thuật

3.4. Các yêu cầu khác:

- **Nhà thầu đề xuất giải pháp, phương pháp luận theo các yêu cầu sau:**

✓ Nhà thầu cung cấp công cụ kiểm soát và quy trình giám sát chất lượng dịch vụ điện toán đám mây, hỗ trợ triển khai bảo mật theo mô hình Zero trust (nếu cần)

✓ Nhà thầu phải minh bạch các vị trí (thành phố, quốc gia) đặt trung tâm dữ liệu bên ngoài lãnh thổ Việt Nam khi triển khai dịch vụ cho Chủ đầu tư;

- **Nhà thầu cam kết các nội dung sau:**

✓ Giải pháp được triển khai trên hạ tầng công nghệ thông tin tương ứng với dịch vụ mà Chủ đầu tư sử dụng đáp ứng các yêu cầu dưới đây:

• Các quy định của pháp luật Việt Nam;

• Có chứng nhận quốc tế còn hiệu lực về bảo đảm an toàn thông tin (nhà thầu đính kèm file chứng nhận quốc tế còn hiệu lực (tính đến thời điểm đóng thầu). Giải pháp phải tối thiểu đạt được các chứng chỉ/chứng nhận quốc tế tương đương còn hiệu lực như sau: (Đính kèm bản chụp và đường dẫn trang web xác nhận của tổ chức đánh giá nếu có):

- ISO 27001 - Quản lý bảo mật thông tin
- ISO 27017 - Hướng dẫn bảo mật thông tin cụ thể cho đám mây
- ISO 27018 - Tiêu chuẩn cụ thể cho đám mây để bảo vệ thông tin nhận dạng cá nhân (PII)

- Chứng nhận tham gia CSA (Cloud Security Alliance): đạt tối thiểu ở mức 1.

✓ Nhà thầu phải cung cấp báo cáo kiểm toán tuân thủ công nghệ thông tin do tổ chức kiểm toán độc lập thực hiện hàng năm trong thời gian thực hiện hợp đồng;

• Trách nhiệm bảo vệ dữ liệu, chống truy cập dữ liệu trái phép trên kênh phân phối dịch vụ từ Nhà thầu đến Chủ đầu tư;

• Dữ liệu của Chủ đầu tư phải được tách biệt với dữ liệu của khách hàng khác sử dụng trên cùng nền tảng kỹ thuật do Nhà thầu cung cấp

✓ Không làm suy giảm khả năng cung cấp dịch vụ liên tục của Chủ đầu tư cho khách hàng.

✓ Không làm suy giảm việc kiểm soát quy trình nghiệp vụ của Chủ đầu tư.

✓ Không làm thay đổi trách nhiệm của Chủ đầu tư trong việc bảo đảm an toàn thông tin.

✓ Dịch vụ công nghệ thông tin của Nhà thầu cung cấp phải đáp ứng các quy định về bảo đảm an toàn thông tin của Chủ đầu tư.

✓ Nhà thầu phải cam kết về việc hỗ trợ truy hồi, di chuyển dữ liệu và phải xóa/tiêu hủy vĩnh viễn toàn bộ dữ liệu của Chủ đầu tư khi hai bên chấm dứt sử dụng dịch vụ

✓ Không sao chép, thay đổi, sử dụng hay cung cấp dữ liệu của Chủ đầu tư cho cá nhân, tổ chức khác (dưới bất kỳ hình thức nào) nếu không được sự đồng ý của Chủ đầu tư

✓ Trong phạm vi cung cấp dịch vụ cho Chủ đầu tư, phải hỗ trợ, hợp tác điều tra trong trường hợp có yêu cầu từ các cơ quan chức năng có thẩm quyền thực hiện xử lý các sự cố vi phạm an toàn thông tin mạng theo quy định của pháp luật. Trường hợp bắt buộc phải cung cấp dữ liệu của Chủ đầu tư cho cơ quan có thẩm quyền (như cơ quan điều tra, phòng chống tội phạm, …) phải thông báo cho Chủ đầu tư

✓ Thông báo cho Chủ đầu tư khi phát hiện cán bộ hoặc hành vi truy cập, sử dụng, tiết lộ, gián đoạn, sửa đổi hoặc phá hoại trái phép, ảnh hưởng đến tính bí mật, tính toàn vẹn và tính sẵn sàng của thông tin đối với dịch vụ mà Chủ đầu tư sử dụng

✓ Trước khi chấm dứt sử dụng dịch vụ, toàn bộ các dữ liệu phát sinh trong quá trình sử dụng dịch vụ của Chủ đầu tư, nhà thầu phải thực hiện:

• Trích xuất và bàn giao cho Chủ đầu tư.

• Sau khi hoàn trả dữ liệu, dữ liệu phải thực hiện xóa. Nhà thầu phải cam kết các dữ liệu không còn được sao lưu, sử dụng ở bất cứ hệ thống nào của nhà thầu, nhà cung cấp Cloud và bên thứ 3 (nếu có)

- **Thời gian hỗ trợ SLA với hỗ trợ kỹ thuật từ nhà thầu:**

Nhà thầu cam kết về SLA với việc hỗ trợ kỹ thuật của nhà thầu cho VietinBank như sau:

- ✓ Trường hợp khẩn cấp: kĩ sư nhà thầu/đối tác phải phản hồi trong vòng 30 phút, cần có mặt onsite tại trụ sở ITC VietinBank trong vòng 60 phút và phối hợp với hãng giải quyết trong thời gian không quá 4 giờ.
- ✓ Các yêu cầu hỗ trợ quan trọng (liên quan hệ thống Production) nhà thầu phải phản hồi trong vòng 60 phút và phối hợp với hãng giải quyết trong thời gian không quá 8 giờ.
- ✓ Các yêu cầu hỗ trợ bình thường: cần phản hồi trong thời gian 2 giờ và giải quyết trong 24 giờ.

Trong đó:

+ **"Trường hợp khẩn cấp":** được hiểu là toàn bộ hệ thống Cloud của VietinBank không thể truy cập được, trong đó bao gồm và không giới hạn các trường hợp lỗi hệ thống của nhà cung cấp Cloud; Các dấu hiệu hiện diện liên quan đến lỗi, nguy cơ ngừng cung cấp các dịch vụ, nguy cơ sai lệch cấu hình của toàn bộ Control Tower/Landing zone/Root account; Các dấu hiệu hiện diện liên quan đến nguy cơ mất an toàn thông tin hệ thống Cloud; Các dấu hiệu hiện diện liên quan đến lộ lọt dữ liệu nhạy cảm, bao gồm và không giới hạn dữ liệu quản trị, dữ liệu người dùng và toàn bộ các loại dữ liệu khác trên Cloud; Các dấu hiệu hiện diện liên quan đến nguy cơ rủi ro cao của hệ thống Cloud của VietinBank; Các dấu hiệu hiện diện liên quan đến phát sinh chi phí lớn nằm ngoài quản lý và mong muốn của VietinBank.
+ **"Trường hợp quan trọng":** được hiểu là các lỗi, sự cố, dấu hiệu phát sinh có liên quan đến các môi trường production của các ứng dụng đang hoạt động trên Cloud; Các dấu hiệu báo hiệu nguy cơ down time của các môi trường production của các ứng dụng đang hoạt động trên Cloud; Các dấu hiệu báo hiệu liên quan đến nguy cơ mất an toàn thông tin hệ thống Cloud; Các dấu hiệu báo hiệu liên quan đến lộ lọt dữ liệu nhạy cảm, bao gồm và không giới

hạn dữ liệu quản trị, dữ liệu người dùng và toàn bộ các loại dữ liệu khác trên Cloud; Các dấu hiệu báo hiệu liên quan đến nguy cơ rủi ro cao của hệ thống Cloud của VietinBank. Các dấu hiệu hiện diện/báo hiệu liên quan đến phát sinh chi phí nhỏ nằm ngoài quản lý và mong muốn của VietinBank.

+ **"Trường hợp bình thường"**: được hiểu là các lỗi, sự cố, dấu hiệu phát sinh liên quan khác không được quy định tại các trường hợp trên.

✓ Các nội dung liên quan đến phân loại các trường hợp có thể được thay đổi tùy theo điều kiện vận hành hệ thống thực tế, hiện trạng và quy định của các văn bản quy phạm pháp luật cũng như các văn bản quy định riêng có liên quan của VietinBank qua từng thời kỳ.

4. Giải pháp và phương pháp luận

Nhà thầu chuẩn bị đề xuất giải pháp, phương pháp luận tổng quát thực hiện dịch vụ theo các nội dung quy định tại Chương này, gồm các phần như sau:

- Giải pháp và phương pháp luận;
- Kế hoạch công tác.

5. Quy định về kiểm tra, nghiệm thu sản phẩm:

- Kết thúc các đợt triển khai, Nhà thầu lập và hoàn thành các biên bản liên quan, lấy xác nhận của các bộ phận, cung cấp đầy đủ các thông tin liên quan phục vụ thanh toán hợp đồng.
- Quy định về thành phần ký các báo cáo, biên bản trong quá trình triển khai sẽ được quy định cụ thể trong hợp đồng với nhà thầu trúng thầu.

6. Quy định trả lời yêu cầu kỹ thuật:

- Nhà thầu cần cung cấp câu trả lời riêng biệt cho mỗi yêu cầu kỹ thuật chi tiết.
- Đối với mỗi yêu cầu, Nhà thầu cần giải thích chi tiết, rõ ràng và cung cấp thông tin, dẫn chứng để tuyên bố đáp ứng (như catalogue, datasheet, hướng dẫn sử dụng,…).
- Trong trường hợp Nhà thầu cung cấp tham chiếu đến các thông tin chi tiết, thông tin tham chiếu phải xác định rõ tên tài liệu, số trang và đoạn tài liệu.
- Để trả lời đối với từng yêu cầu, đề nghị Nhà thầu sử dụng Bảng mẫu Trả lời dưới đây:

Stt	Yêu cầu	Mức độ đáp ứng	Dẫn chứng trong E-HSDT

		(chọn Đáp ứng/ Không đáp ứng)	
[Yêu cầu trong E-HSMT]	Yêu cầu: [đưa phần mô tả yêu cầu từ E- HSMT]		Chỉ dẫn tới dẫn chứng trong E-HSDT

- Nhà thầu phải nêu rõ đã giải thích/dẫn chứng tại phần nào, mục nào, tài liệu nào của E-HSDT, đáp ứng yêu cầu kỹ thuật gì trong E-HSMT, để bên mời thầu dễ dàng tham chiếu khi xem xét E-HSDT.

- Trường hợp E-HSDT thiếu các tài liệu theo yêu cầu, hoặc nhà thầu chỉ dẫn, dẫn chiếu không đúng, hoặc thông tin trong E-HSDT được trích dẫn không chính xác, hoặc thông tin trong E-HSDT không được tìm thấy trên các địa chỉ của chính hãng cung cấp sản phẩm, dịch vụ, hoặc không có cơ sở để cho rằng sản phẩm, dịch vụ dự thầu có cấu hình tương đương hoặc đáp ứng yêu cầu kỹ thuật trong E-HSMT thì Chủ đầu tư sẽ yêu cầu nhà thầu làm rõ E-HSDT trên cơ sở tuân thủ quy định tại Mục 23 E-CDNT