

## Phần 2. YÊU CẦU VỀ KỸ THUẬT

### Chương V. Yêu cầu về kỹ thuật

#### 1. Phạm vi cung cấp

STT	Nội dung	Số lượng	Mô tả/Ghi chú
1	Bản quyền phần mềm Hệ thống Quản lý đào tạo tổng thể - LMS trong thời hạn 3 năm.	- Năm 1: 23.000 user - Năm 2: 24.000 user - Năm 3: 25.000 user	Tính từ ngày go-live hệ thống
2	Dịch vụ triển khai hệ thống, tích hợp và đào tạo	01 gói	Trong 6 tháng kể từ ngày hợp đồng có hiệu lực

#### 2. Thời gian thực hiện hợp đồng

43 tháng kể từ khi hợp đồng có hiệu lực, trong đó:

- Triển khai cài đặt, đào tạo: trong 6 tháng, kể từ ngày hợp đồng có hiệu lực;
- Thời gian cung cấp bản quyền: 36 tháng, kể từ ngày go-live hệ thống;
- Thời gian nghiệm thu, thanh lý hợp đồng: 01 tháng, kể từ ngày kết thúc thời gian cung cấp bản quyền.

#### 3. Tiêu chuẩn kỹ thuật phần mềm

A	CÁC YÊU CẦU KỸ THUẬT
<b>I. Yêu cầu chung</b>	
1	Hệ thống là 100% web-based (các chức năng, module truy cập được thông qua trình duyệt web) và ứng dụng trên thiết bị di động.
2	Hệ thống cho phép truy cập hệ thống từ các thiết bị di động khác nhau: desktop/laptop/tablet/mobile. Hỗ trợ hiển thị giao diện tối ưu trên các thiết bị di động chạy hệ điều hành Android, iOS.
3	Tương thích các trình duyệt web, tối thiểu: Firefox từ 132.0 trở lên, Chrome từ 131.0 trở lên, Safari từ 17.6 trở lên, Microsoft Edge từ 142 trở lên
4	Hệ thống hỗ trợ số lượng lớn người truy cập (tối thiểu 2.500 lượt truy cập đồng thời)
5	Hệ thống cung cấp chức năng tìm kiếm đảm bảo hỗ trợ tìm kiếm gần đúng theo cụm từ, tìm kiếm chính xác
<b>II. Giao diện người sử dụng</b>	
6	Hệ thống cho phép cập nhật giao diện theo nhận diện thương hiệu riêng của BIDV từng thời kỳ
7	Ngôn ngữ của giao diện người sử dụng là tiếng Việt và tiếng Anh
<b>III. Quản trị Người sử dụng</b>	
<b>III.1 Quản lý tổ chức, bao gồm các chức năng:</b>	
8	Tạo số lượng tổ chức (Phòng Ban, Công ty con) không hạn chế
9	Xem, phê duyệt đăng ký học tập của các thành viên trong tổ chức
10	Cập nhật, thay đổi người quản lý tổ chức
<b>III.2 Quản lý học viên/người sử dụng, bao gồm các chức năng:</b>	

11	Khởi tạo, chỉnh sửa các user truy cập hệ thống với các thông tin cơ bản sau: Tên đăng nhập, mật khẩu đăng nhập, họ tên, chức danh, giới tính, email, trạng thái tài khoản (tối thiểu “đang sử dụng” hay “dừng hoạt động”), ngày hết hạn sử dụng hệ thống, ngày sinh.
12	Khởi tạo người sử dụng theo lô
13	Phân quyền cho các đối tượng khác nhau, tối thiểu gồm: Quản trị viên, Quản lý đào tạo, Giảng viên, học viên
<b>IV. Quản lý khóa học</b>	
<b>IV.1 Quản lý khóa học (chung cho các loại hình), bao gồm các chức năng:</b>	
14	Tạo mới/sửa/xóa các danh mục khóa học, danh mục khóa học được tổ chức dưới dạng cây thư mục
15	Tổ chức lớp học kết hợp (gồm cả đào tạo tập trung và đào tạo trực tuyến)
16	Thiết lập các thông tin chung của khóa học, tối thiểu: tên khóa học, ngày bắt đầu, ngày kết thúc, thông tin của tất cả các học viên đã đăng ký khóa học
17	Upload đa dạng các tài liệu, tối thiểu: File Word, pdf, excel, ppt, video, bài giảng đóng gói theo chuẩn quốc tế (Scorm, AICC, Tincan)
18	Thiết lập các điều kiện tiên quyết để hoàn thành khóa học
19	Gán các bài kiểm tra cho khóa học: Gán/xóa các bài kiểm tra cho khóa học, cung cấp chức năng cho người quản trị thiết lập lựa chọn số lần làm bài kiểm tra.
20	Tạo check list gồm những thông tin cơ bản như: ngày giờ diễn ra, điểm số, nhận xét, file đính kèm
21	Gán/gỡ bỏ giáo viên quản lý khóa học
22	Gán đánh giá cho khóa học, đánh giá giảng viên theo từng buổi học hoặc cả khóa học
23	Thiết lập các chính sách đăng ký khóa học. Giới hạn học viên được đăng ký khóa học
24	Tìm kiếm các học viên đang tham gia khóa học đó
25	Gửi thông báo tự động cho học viên trên hệ thống (notification) hoặc qua Email theo yêu cầu người quản lý ví dụ: phê duyệt đăng ký học tập, thông báo tham gia khóa học, thông báo hoàn thành khóa học
26	Xem lịch đào tạo (để học viên chủ động tham dự)
27	Tạo ra các diễn đàn thảo luận. Diễn đàn này sẽ được gán cho các khóa đào tạo để học viên và giáo viên trao đổi thông tin
<b>IV.2 Quản lý khóa học tập trung, bao gồm các chức năng:</b>	
28	Thiết lập thời khóa biểu, các buổi học cho khóa học theo kế hoạch học tập cụ thể
29	Thiết lập điểm danh QRcode trong khóa học
30	Cho phép học viên tự điểm danh QRcode
31	Cho phép giảng viên điểm danh tại lớp học
32	Gán/gỡ bỏ giáo viên cho mỗi module học
<b>V. Quản lý câu hỏi, kiểm tra</b>	
<b>V.1 Ngân hàng câu hỏi, bao gồm các chức năng:</b>	
33	Tạo, phân quyền truy cập danh mục câu hỏi
34	Upload câu hỏi với số lượng không hạn chế
35	Thêm mới/Sửa/Xóa câu hỏi
36	Hỗ trợ nhiều dạng câu hỏi khác nhau, tối thiểu: Câu hỏi Đúng/Sai, câu hỏi 1 lựa chọn, câu hỏi nhiều lựa chọn, câu hỏi tự luận cho phép chấm điểm, câu hỏi có câu trả lời bằng chữ, Câu hỏi bằng hình ảnh

37	Thiết lập điểm số cho mỗi câu hỏi
38	Xem trước câu hỏi
39	Chèn các file hình ảnh vào mỗi câu hỏi
40	Nhập câu hỏi lên hệ thống tối thiểu từ file Excel
<b>V.2 Biên tập bài kiểm tra, bao gồm các chức năng:</b>	
41	Thêm mới/Sửa/Xóa bài kiểm tra
42	Mô tả bài nội dung bài kiểm tra
43	Thiết lập thời gian bài kiểm tra
44	Thiết lập số lần làm bài kiểm tra
46	Thiết lập điểm hoàn thành cho bài kiểm tra
47	Tạo nội dung kiểm tra theo các học phần
48	Người quản trị xem trước bài kiểm tra
49	Tạo bài kiểm tra bằng cách chọn các câu hỏi cụ thể hoặc chọn ngẫu nhiên từ ngân hàng câu hỏi
50	Tạo bài kiểm tra trắc nghiệm và bài kiểm tra luận và cung cấp chức năng cho phép chấm điểm lại.
51	Cho phép đáp án câu hỏi được đảo vị trí ngẫu nhiên hoặc theo thứ tự đặt trước
52	Hiển thị kết quả câu trả lời sau khi học viên hoàn thành bài kiểm tra
<b>V.3 Quản lý đánh giá hiệu quả đào tạo, bao gồm các chức năng:</b>	
53	Quản lý, triển khai và theo dõi hoạt động đánh giá hiệu quả đào tạo theo mô hình Kirkpatrick hoặc Phillips, tối thiểu đến cấp độ 3 (Hành vi/Ứng dụng, bảo đảm đo lường được mức độ thay đổi hành vi và khả năng vận dụng kiến thức, kỹ năng của học viên sau đào tạo)
<b>VI. Quản lý chứng chỉ và Hồ sơ học tập, bao gồm các chức năng:</b>	
54	Người quản trị tự định nghĩa, sửa, xóa các yêu cầu năng lực theo từng vị trí
55	Nhập mô hình hồ sơ năng lực có sẵn từ file excel
56	Tạo, thay đổi các mô hình hồ sơ năng lực
57	Định nghĩa và quản lý chức danh (job title)
58	Duy trì kết nối chức danh (job title) với kỹ năng/hồ sơ năng lực. Các chức danh do người quản trị thiết lập theo thông tin chức danh của tổ chức
59	Gán, loại bỏ các kỹ năng vào hồ sơ năng lực
60	Kết nối hồ sơ năng lực, yêu cầu theo từng vị trí chức danh với các khoá học, bài kiểm tra.
61	Ghi nhận các chứng nhận cá nhân tự đào tạo làm cơ sở đánh giá năng lực theo vị trí công việc của người dùng: Ví dụ chứng chỉ Anh (TOEIC, IELTS,...), hoặc các chứng chỉ khác
62	Đưa ra lộ trình đào tạo cho người dùng theo chức danh người dùng đăng ký
63	Quản lý và theo dõi kỹ năng và hồ sơ năng lực của từng học viên. Phân tích các kỹ năng còn thiếu của học viên dựa trên chức danh
64	Hiển thị các khoá học cho mỗi học viên dựa trên chức danh công việc
65	Theo dõi tiến trình hoàn thành lộ trình học tập của học viên. Cán bộ đào tạo có thể xem từng cá nhân, từng đơn vị, từng vị trí
66	Tạo kế hoạch học tập, deadline cho lộ trình học tập
67	Cập nhật cấp độ năng lực của học viên sau đào tạo/theo định kỳ
<b>VI. 4 Quản lý chứng chỉ, bao gồm các chức năng:</b>	
68	Tạo và gán chứng chỉ cho khóa học
69	In chứng chỉ
<b>VII. Ứng dụng trí tuệ nhân tạo (AI) trong các chức năng:</b>	

70	Hỗ trợ gợi ý học tập cá nhân hóa: AI phân tích kỹ năng, chức danh, lịch sử học tập và hành vi người dùng để tự động đề xuất khóa học phù hợp nhất. Đề xuất lộ trình học tập theo mục tiêu nghề nghiệp và khung năng lực
71	Hỗ trợ tự động phát hiện khoảng trống kỹ năng và đề xuất nội dung học viên cần học để cải thiện
72	Hỗ trợ tìm kiếm dựa trên ngữ nghĩa, cho phép người dùng tìm nội dung chính xác dù nhập từ khóa không rõ ràng. Tự động gắn thẻ nội dung (auto-tagging) giúp quản trị nội dung dễ dàng hơn
73	Hỗ trợ nhận diện xu hướng, mức độ tương tác và mức độ phù hợp để gợi ý nội dung mới, giúp danh mục đào tạo luôn cập nhật và giảm tải công việc cho quản trị viên
74	Hỗ trợ dự đoán người học có nguy cơ không hoàn thành, nội dung có mức độ tương tác thấp và xu hướng phát triển năng lực.
<b>VIII. Quản lý chi phí</b>	
75	Hệ thống cung cấp chức năng quản lý ngân sách đào tạo, khởi tạo ngân sách theo năm cho từng bộ phận, ngân sách có thể phân bổ theo người học
76	Hệ thống cung cấp chức năng quản lý, ghi nhận chi phí cho các khóa học bên ngoài và bên trong
<b>IX. Lớp học ảo, bao gồm các chức năng:</b>	
77	Tích hợp với các hệ thống lớp học ảo phổ biến như: Zoom, webex, hoặc tương đương
78	Tạo và tham gia lớp học ảo ngay trong hệ thống
79	Cho phép tự động điểm danh với các học viên tham gia, người quản lý có thể cấu hình điều kiện tham gia tối thiểu bao nhiêu % thời lượng lớp học. Khi học viên tham gia đủ thời gian tối thiểu, hệ thống sẽ tự động ghi nhận là hoàn thành lớp học
80	Gán giáo viên hướng dẫn vào lớp học ảo
<b>X. Ứng dụng trên thiết bị di động, bao gồm các chức năng:</b>	
81	Ứng dụng phục vụ học trên thiết bị di động được cập nhật thường xuyên để đáp ứng sử dụng trên hệ điều hành mới và tối thiểu đáp ứng: - Hỗ trợ từ Android 6 và iOS 12 trở lên - Được triển khai trên public store như Google Play và Apple Store.
82	Cho học viên đăng ký tham dự các khóa học và theo dõi trạng thái phê duyệt tham dự các khóa học đã đăng ký
83	Học viên xem các thông báo (notification) từ hệ thống hoặc người quản trị
84	Học viên tải khóa học và học offline; đồng bộ lại quá trình học tập khi có kết nối mạng
85	Học viên xem tài liệu, video, bài giảng đã số hóa, làm bài kiểm tra, bài khảo sát và thực hiện điểm danh bằng QR code
86	Học viên theo dõi kết quả học tập tại lớp học
87	Ứng dụng cần đảm bảo các tiêu chuẩn liên quan đến bảo mật cho ứng dụng di động, tối thiểu bao gồm: - Chống dịch ngược - Chống Overlay - Chống đóng gói lại ứng dụng - Phát hiện thiết bị root/ jailbreak - Phát hiện môi trường giả lập (Emulator Detection)

	- Hỗ trợ Anti- debugging
<b>XI. Học tập mở, bao gồm các chức năng:</b>	
88	Cung cấp đa dạng hình thức học tập như: Thông qua khóa học, bài giảng ngắn (video, bản tin – podcast, sách nói, ebook...), qua các bài kiểm tra nghiệp vụ có sẵn
89	Xếp hạng học viên học viên căn cứ theo cấu hình điểm số nhận được khi hoàn thành các nội dung học tập trên hệ thống
<b>XII. Quản lý báo cáo, bao gồm các chức năng:</b>	
90	Tạo ra các loại báo cáo động tùy biến theo nhu cầu của người sử dụng bao gồm ít nhất các tính năng: - Cung cấp đa dạng cách thức lọc kết quả hiển thị như: + Ngày bắt đầu tổ chức, ngày kết thúc; + Tên khóa học, phòng ban, đơn vị, vị trí; - Thống kê kết quả học tập, chi phí: + Thống kê chi tiết số lượng khóa học đã/đang hoàn thành, thời lượng học, điểm số, tỷ lệ hoàn thành theo từng học viên, nhóm đối tượng, vị trí... + Tình trạng hoàn thành các khóa học bắt buộc theo thời hạn, giúp đảm bảo tuân thủ yêu cầu đào tạo nội bộ; + Thống kê kết quả học tập theo vị trí chức danh theo học viên; + Thống kê học viên tham gia học tập trên hệ thống theo thời gian; + Thống kê số lần tương tác của người học với nội dung bài học; thời lượng mà một học viên sử dụng để hoàn thành một nhiệm vụ, chủ đề hay một phần khóa học/bài giảng; tổng thời lượng mà mỗi học viên sử dụng để hoàn thành khóa học; + Tổng hợp chi phí theo khóa học, chương trình, đơn vị, người học. Báo cáo sau khi tạo ra sẽ được lưu lại thành các mẫu để được sử dụng về sau hoặc lập lịch tạo báo cáo định kỳ
91	Cung cấp định dạng dữ liệu file đầu ra của báo cáo là dạng file tối thiểu Excel, pdf.
92	Cung cấp báo cáo dạng đồ thị, hình ảnh để quản trị viên và người quản lý có được cái nhìn tổng quan về tiến độ đào tạo, các bản đánh giá và chương trình tuân thủ như: - Dashboard thể hiện ma trận học tập của từng học viên, bao gồm tiến độ hoàn thành các khóa học, sơ đồ hóa lộ trình học tập và trạng thái đáp ứng các yêu cầu đào tạo; - Biểu đồ đối chiếu chi phí thực tế với ngân sách kế hoạch; biểu đồ hiển thị xu hướng chi phí theo thời gian
93	Phân quyền cho những người sử dụng được phép tạo báo cáo (Cán bộ đầu mối đào tạo, cán bộ quản lý tại đơn vị, học viên...)

#### 4. Các yêu cầu kỹ thuật khác

<b>B</b>	<b>CÁC YÊU CẦU KỸ THUẬT KHÁC</b>
<b>I</b>	<b>Yêu cầu thanh toán user sử dụng, bản quyền, hỗ trợ điều tra</b>
1	BIDV chỉ thanh toán chi phí đối với những tài khoản người dùng (user) có phát sinh hoạt động học tập thực tế trên hệ thống (tham gia khóa học, xem video, đọc tài liệu thực tế). Các trường hợp tài khoản chỉ khởi tạo hoặc có truy cập nhưng không tham gia học tập sẽ không bị tính phí. Căn cứ thanh toán sẽ dựa trên dữ liệu trích xuất từ báo cáo hệ thống và phải được đại diện hai bên ký xác nhận

2	Bản quyền: Trong trường hợp nhà thầu sử dụng giải pháp, phần mềm hoặc dịch vụ từ bên thứ ba, nhà thầu phải đảm bảo rằng việc sử dụng đó không vi phạm bản quyền và đã được cấp phép hợp lệ. Nhà thầu có trách nhiệm đảm bảo BIDV không bị khiếu kiện, yêu cầu bồi thường liên quan đến vi phạm sở hữu trí tuệ từ bên thứ ba
3	Hỗ trợ điều tra: Nhà thầu cam kết phối hợp với Nhà cung cấp dịch vụ Cloud 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. Trong trường hợp bắt buộc phải cung cấp dữ liệu của BIDV cho cơ quan có thẩm quyền (như cơ quan điều tra, phòng chống tội phạm, ...), phải thông báo cho BIDV và được BIDV chấp thuận trước khi thực hiện
<b>II</b>	<b>Yêu cầu đối với nhà cung cấp dịch vụ Cloud</b>
4	Có chứng nhận quốc tế còn hiệu lực về đảm bảo an toàn thông tin, tối thiểu ISO 27001, SOC2 hoặc tương đương.
5	Cam kết về quyền sử dụng các sản phẩm sở hữu trí tuệ, bản quyền liên quan trực tiếp đến dịch vụ Cloud và trách nhiệm của Nhà cung cấp đối với các quyền này khi cung cấp cho BIDV
<b>III</b>	<b>Yêu cầu về tích hợp</b>
6	<p>Có khả năng đáp ứng các yêu cầu tích hợp như sau:</p> <ul style="list-style-type: none"> <li>- Đối với hệ thống bên trong BIDV: Tích hợp hệ thống bên trong của BIDV thông qua giao thức API (RESTful), đồng bộ dữ liệu và tích hợp file, các hệ thống nội bộ gồm: <ul style="list-style-type: none"> <li>o Hệ thống xác thực và phân quyền người dùng (One Access) để cấp phát phiên truy cập và đăng nhập một lần (SSO) cho phép người dùng chỉ cần đăng nhập 1 lần để truy cập các hệ thống nội bộ của BIDV.</li> <li>o Hệ thống kho dữ liệu tập trung (MIS) để đồng bộ mô hình tổ chức và thông tin người dùng.</li> <li>o Hệ thống quản trị nhân sự để lấy thông tin khóa học từ quản lý nhân sự và đồng bộ học viên tham dự, kết quả học tập, kết quả đánh giá từ LMS về quản lý nhân sự.</li> </ul> </li> <li>+ Trách nhiệm của các bên như sau: <ul style="list-style-type: none"> <li>o Nhà thầu có trách nhiệm xây dựng phương án, thực hiện tích hợp (phát triển module, bàn giao và phối hợp triển khai).</li> <li>o BIDV phối hợp cung cấp dữ liệu, hạ tầng và đầu mối triển các cấu phần trên hạ tầng của BIDV.</li> </ul> </li> <li>- Nhà thầu phải thực hiện tích hợp hệ thống với các nền tảng, nhà cung cấp dịch vụ đào tạo trực tuyến uy tín và nền tảng lớp học ảo để phục vụ công tác đào tạo, bao gồm tối thiểu: <ul style="list-style-type: none"> <li>+ Tích hợp với các nền tảng khóa học trực tuyến (như Udemy, Coursera hoặc tương đương): <ul style="list-style-type: none"> <li>o Đồng bộ thông tin khóa học.</li> <li>o Cho phép cán bộ BIDV truy cập và học tập trực tiếp thông qua hệ thống LMS.</li> <li>o Việc tích hợp phải được thực hiện thông qua API hoặc các giao thức kết nối tiêu chuẩn do nhà cung cấp bên thứ ba cung cấp.</li> </ul> </li> <li>+ Tích hợp với nền tảng lớp học ảo (tối thiểu: Webex): <ul style="list-style-type: none"> <li>o Cho phép tạo và tham gia lớp học ảo từ hệ thống LMS.</li> <li>o Việc tích hợp phải được thực hiện thông qua API hoặc các giao thức kết</li> </ul> </li> </ul> </li> </ul>

	nổi tiêu chuẩn do nhà cung cấp nền tảng lớp học ảo cung cấp.
7	<p>Yêu cầu về đặc điểm tích hợp:</p> <ul style="list-style-type: none"> <li>- Phương thức tích hợp: API, Event/Message, File, ... Kiến trúc tích hợp phải đảm bảo việc tích hợp giữa các phần mềm và các dịch vụ.</li> <li>- Giao thức tích hợp: RESTful, event/message, tích hợp file, tích hợp dữ liệu</li> </ul>
<b>IV</b>	<b>Yêu cầu về an toàn bảo mật</b>
<b>IV.1</b>	<b>Yêu cầu mạng kết nối</b>
8	<p>Yêu cầu về các kết nối: Kết nối vào/ra từ Internet.</p> <ul style="list-style-type: none"> <li>- Việc kết nối hệ thống LMS với Internet phải được kiểm soát chặt chẽ thông qua các thiết bị và giải pháp an ninh mạng phù hợp, đảm bảo chỉ các dịch vụ, công kết nối và giao thức được phê duyệt mới được phép truy cập</li> <li>- Hệ thống phải được triển khai các cơ chế bảo vệ nhằm phòng chống các mối đe dọa tấn công từ Internet như tấn công từ chối dịch vụ, khai thác lỗ hổng ứng dụng và các hình thức tấn công phổ biến khác</li> <li>- Lưu lượng truy cập vào/ra Internet phải được giám sát, ghi nhận nhật ký (log) và lưu trữ theo quy định, phục vụ công tác giám sát an toàn thông tin, đánh giá rủi ro và xử lý sự cố khi phát sinh</li> </ul>
9	<p>Yêu cầu về phân vùng, phân đoạn mạng:</p> <ul style="list-style-type: none"> <li>- Hệ thống LMS phải được thiết kế và triển khai theo kiến trúc mạng phân vùng, đảm bảo tách biệt rõ ràng giữa các vùng mạng có mức độ tin cậy khác nhau (ví dụ: Internet, DMZ, mạng ứng dụng, mạng cơ sở dữ liệu, mạng quản trị)</li> <li>- Việc kết nối giữa các vùng mạng phải được kiểm soát thông qua các thiết bị an ninh mạng chuyên dụng (Firewall/WAF/IPS hoặc tương đương), áp dụng nguyên tắc chỉ cho phép các luồng kết nối cần thiết (least privilege), hạn chế tối đa kết nối trực tiếp, không kiểm soát giữa các vùng mạng</li> <li>- Các chính sách mạng phải cho phép giám sát, ghi log và truy vết các kết nối phục vụ công tác vận hành, giám sát an toàn thông tin và điều tra sự cố khi cần thiết</li> </ul>
10	<p>Yêu cầu về quy hoạch, tách biệt tài nguyên của BIDV trên môi trường của NCC</p> <ul style="list-style-type: none"> <li>- Tách biệt với các môi trường mạng với khách hàng khác</li> <li>- Tách biệt dữ liệu của BIDV với các khách hàng sử dụng dịch vụ SaaS</li> </ul>
<b>IV.2</b>	<b>Yêu cầu về bảo mật hạ tầng</b>
11	Nhà cung cấp phải đảm bảo máy chủ ảo triển khai LMS đã được hardening theo tiêu chuẩn quốc tế như: CIS Benchmark hoặc NIST, hoặc các tiêu chuẩn tương đương
12	Nhà cung cấp phải đảm bảo yêu cầu về bảo mật bộ nhớ trên môi trường Cloud dữ liệu của BIDV trên hạ tầng LMS phải được mã hoá at-rest bằng AES-256
13	Nhà cung cấp phải đảm bảo công tác scan lỗ hổng (VA) container/image định kỳ, cảnh báo cho BIDV và khắc phục các lỗ hổng mức độ trung bình trở lên (tham chiếu thang điểm CVSS 3.1/4.0)
<b>IV.3</b>	<b>Quản lý xác thực người dùng và phiên đăng nhập</b>

14	Hệ thống hỗ trợ xác thực đăng nhập vào hệ thống thông qua xác thực đa yếu tố (MFA), tối thiểu áp dụng cho tài khoản quản trị; các tài khoản khác bắt buộc đăng nhập bằng tài khoản & mật khẩu
15	Hệ thống cung cấp chức năng quản lý thời gian hết hạn phiên làm việc (session timeout). Thời gian chờ tối đa cho mỗi phiên đăng nhập, trong trường hợp người sử dụng không phát sinh thao tác, mặc định là 15 phút. Khi phiên làm việc hết hạn, hệ thống phải yêu cầu người sử dụng thực hiện đăng nhập lại để tiếp tục sử dụng. Hệ thống cho phép quản trị viên cấu hình, điều chỉnh thời gian hết hạn phiên theo chính sách quản lý và yêu cầu vận hành của đơn vị.
<b>IV.4</b>	<b><i>Yêu cầu bảo mật mạng</i></b>
16	- Có chức năng tường lửa để kiểm soát các kết nối, truy cập vào ra vùng mạng quan trọng
17	Các luật kiểm soát kết nối trên tường lửa (firewall) phải đảm bảo các nguyên tắc sau: - Phải có luật chặn mặc định các kết nối mạng không cần thiết (Luật deny- all được thiết lập mặc định cho kiểm soát trên firewall). Kết nối được mở được dựa trên phân quyền, sự cho phép và phù hợp với chức năng, yêu cầu công việc. - Các đối tượng địa chỉ nguồn, đích và các cổng kết nối phải được xác định cụ thể không được sử dụng luật "Any to any" hoặc mở thừa so với yêu cầu thực tế.
18	Đảm bảo chống tấn công từ chối dịch vụ phân tán (DDoS) ở lớp mạng
<b>IV.4</b>	<b><i>Yêu cầu bảo mật ứng dụng</i></b>
19	Có chứng nhận quốc tế còn hiệu lực về đảm bảo an toàn thông tin như ISO 27001, SOC 2 hoặc tương đương
20	Hệ thống được cung cấp phải được thực hiện đánh giá an toàn thông tin định kỳ tối thiểu 01 lần/năm qua email bởi tổ chức đánh giá độc lập, có năng lực và được cấp phép theo quy định pháp luật. Báo cáo đánh giá cần bao gồm nội dung kiểm thử lỗ hổng bảo mật (vulnerability assessment, penetration testing) và kết quả xử lý: tất cả các lỗ hổng được phát hiện đều phải có phương án khắc phục, cập nhật bản vá hoặc biện pháp kiểm soát rủi ro phù hợp.
21	Hệ thống đảm bảo được bảo vệ chống tấn công từ chối dịch vụ (DDoS)
22	Hệ thống đảm bảo được bảo vệ bởi tường lửa ứng dụng web (Web application firewall - WAF), WAF hỗ trợ bảo vệ tối thiểu khỏi các lỗ hổng bảo mật theo OWASP Top 10
23	Hệ thống đảm bảo được bảo vệ tấn công bởi bot
24	Hệ thống đảm bảo được kiểm soát quyền truy cập vào API với tối thiểu các cơ chế: Rate limit, Token-Based Access
25	Hệ thống được bảo vệ bởi các hình thức tấn công API cơ bản: Injection, Broken Authentication, SSRF, ...
26	Hệ thống được bảo vệ khỏi tất cả các hình thức tấn công phổ biến gồm: SQL Injection, cross-site scripting, command injection, HTTP hi-jacking, HTTP protocol violation, crawler
27	Hệ thống được bảo vệ khỏi nguy cơ rò rỉ, đánh cắp dữ liệu (Page, script defense)

28	Nhà thầu phải thuê bên thứ ba đánh giá bảo mật độc lập (là tổ chức được cơ quan có thẩm quyền cấp phép về dịch vụ đánh giá bảo mật) theo hình thức Graybox và đảm bảo khắc phục toàn bộ các lỗ hổng bảo mật tìm được (nếu có) trong vòng 6 tháng trước khi triển khai. Toàn bộ chi phí thuê đánh giá bảo mật do nhà thầu chi trả. Bằng chứng về kết quả đánh giá bảo mật phải được cung cấp cho BIDV.
29	Hệ thống hỗ trợ đẩy log về hệ thống SIEM (Qradar) & SOAR(Cortex xSOAR) của BIDV phục vụ giám sát, phân tích, điều tra sự kiện bảo mật
<b>IV.5</b>	<b>Bảo mật về dữ liệu</b>
30	Dữ liệu truyền/nhận giữa môi trường Cloud cung cấp cho BIDV và các môi trường khác phải bảo đảm: tính bí mật và phải được truyền đầy đủ, đúng địa chỉ; Có biện pháp bảo vệ phòng chống các thay đổi hoặc sao chép, sử dụng trái phép.
31	Các dữ liệu của BIDV lưu trữ trên môi trường Cloud phải đảm bảo: Có phương án phân quyền đảm bảo các quyền xem/sửa/xóa/tải dữ liệu theo yêu cầu cụ thể
32	Dữ liệu ở trạng thái lưu trữ (at rest) và truyền tải (in transit) phải được mã hóa mạnh (tương đương hoặc cao hơn AES-256 hoặc TLS 1.2+)
33	Cam kết thực hiện các yêu cầu liên quan để đảm bảo tuân thủ quy định của Pháp luật về bảo vệ dữ liệu cá nhân và tuân thủ quy định pháp luật liên quan của Việt Nam.
34	Hệ thống LMS phải thực hiện xác thực người dùng thông qua việc kết nối, gọi xác thực trực tiếp tới hệ thống OneAccess/AD của BIDV theo cơ chế SSO, không yêu cầu đồng bộ, sao chép hay lưu trữ dữ liệu định danh người dùng của BIDV sang hệ thống Cloud. Việc xác thực phải tuân thủ các chính sách quản lý truy cập và an toàn thông tin hiện hành của BIDV
<b>IV.6</b>	<b>Yêu cầu về tự động phát hiện, điều tra các mối đe dọa, lỗ hổng bảo mật</b>
35	Nhà cung cấp phải chịu chi phí trang bị và sử dụng chứng chỉ SSL thương mại cho hệ thống
36	Nhà thầu cam kết xử lý triệt để các lỗ hổng bảo mật đã được công bố, mã lỗi có khả năng gây thiệt hại cho hệ thống của BIDV trong suốt quá trình sử dụng. Khi phát hiện các lỗ hổng ảnh hưởng ở mức cao, nghiêm trọng, nhà thầu phải thực hiện ngay các biện pháp cập nhật, khắc phục, giảm thiểu rủi ro cho nền tảng trong vòng 24h. Đối với các lỗ hổng còn lại, thời gian khắc phục không quá 7 ngày kể từ ngày phát hiện. Trong đó: Rủi ro mức cao là rủi ro có thể gây ảnh hưởng lớn đến hoạt động đào tạo như hệ thống ngừng hoạt động, mất dữ liệu một phần, gián đoạn chương trình đào tạo; Rủi ro mức nghiêm trọng là rủi ro có thể gây ảnh hưởng nghiêm trọng đến hoạt động đào tạo như hệ thống ngừng hoạt động và không thức khắc phục ngay, mất dữ liệu trên diện rộng.
<b>V</b>	<b>Yêu cầu về dữ liệu</b>
<b>V.1</b>	<b>Yêu cầu về quyền sở hữu, chủ quyền dữ liệu:</b>
37	Quyền sở hữu: dữ liệu trên phần mềm là của BIDV trong toàn bộ vòng đời dữ liệu
38	Chủ quyền dữ liệu: Dữ liệu thuộc sở hữu BIDV
<b>V.2</b>	<b>Bảo vệ, sửa đổi, sao lưu CSDL</b>
39	Hệ quản trị CSDL của hệ thống phải có cơ chế bảo vệ và phân quyền truy cập đối với các tài nguyên CSDL. Thực hiện phân quyền với từng cá nhân truy cập đến CSDL

40	<p>Nhà cung cấp phải có các biện pháp phát hiện, ngăn chặn các hình thức tấn công CSDL và phải có các biện pháp thích hợp để đảm bảo dữ liệu thuộc CSDL được lưu trữ an toàn, đầy đủ, toàn vẹn và chính xác theo nguyên tắc: - Tất cả dữ liệu, thông tin lưu trong CSDL phải được lưu trữ một cách an toàn và phải được bảo vệ khỏi mọi nguy cơ bị sửa đổi, truy cập trái phép hoặc rò rỉ; Đảm bảo thông tin trong CSDL được an toàn bảo mật, toàn vẹn, đầy đủ, không bị thay đổi, sai lệch trong suốt thời gian lưu trữ.</p> <p>- Áp dụng các biện pháp kỹ thuật, công nghệ cần thiết để phát hiện và ngăn chặn những trường hợp truy cập trái phép vào CSDL; Đảm bảo chỉ những cá nhân có thẩm quyền mới được phép tiếp cận đến dữ liệu của CSDL</p>
41	<p>Lưu trữ dữ liệu đào tạo của BIDV trên nền tảng Cloud</p> <p>- Đơn vị cung cấp giải pháp cam kết bảo vệ, bảo mật dữ liệu của BIDV theo quy định của pháp luật. Đảm bảo dữ liệu của BIDV được tách biệt, không bị chia sẻ, không bị truy cập hoặc sử dụng trái phép bởi nhà cung cấp dịch vụ hoặc khách hàng khác</p> <p>- Thời gian lưu trữ dữ liệu: Trong suốt quá trình triển khai dự án (dự kiến 6 tháng triển khai, 3 năm thuê bản quyền) và cho đến khi thực hiện bàn giao lại toàn bộ dữ liệu cho BIDV</p>
42	<p>Nhà cung cấp đảm bảo việc backup dữ liệu:</p> <p>- Loại dữ liệu được backup: toàn bộ.</p> <p>- Dữ liệu backup về khu vực lưu trữ của nhà cung cấp.</p> <p>- Tần suất đồng bộ dữ liệu định kỳ 1 tuần/lần</p>
43	<p>Nhà cung cấp đảm bảo việc kiểm soát chất lượng dữ liệu, mức độ sử dụng dữ liệu được chính xác và nhất quán</p>
44	<p>Cung cấp cho BIDV bản sao dữ liệu của BIDV trên Cloud khi được yêu cầu, tối thiểu gồm: dữ liệu, nhật ký truy cập cơ sở dữ liệu và nhật ký truy cập dịch vụ.</p>
<b>V.3</b>	<b><i>Sử dụng dữ liệu</i></b>
45	<p>Nhà thầu cam kết chỉ BIDV có quyền khai thác, chia sẻ, phân phối dữ liệu. Không sao chép, thay đổi, sử dụng hay cung cấp dữ liệu của BIDV cho cá nhân, tổ chức khác, trừ trường hợp có yêu cầu của cơ quan nhà nước có thẩm quyền theo quy định của pháp luật; trong trường hợp này, bên thứ ba phải thông báo cho BIDV trước khi cung cấp dữ liệu, trừ khi việc thông báo sẽ vi phạm pháp luật Việt Nam;</p>
46	<p>Trường hợp xóa dữ liệu:</p> <p>- Đảm bảo dữ liệu được xóa phù hợp với vòng đời dữ liệu và khi BIDV không còn sử dụng dịch vụ của nhà cung cấp. Biện pháp xóa dữ liệu: xóa logic, xóa vật lý, xóa không thể phục hồi</p> <p>- Dữ liệu phát sinh trong quá trình sử dụng dịch vụ là tài sản của BIDV. Khi chấm dứt sử dụng dịch vụ:</p> <p>+ Nhà thầu thực hiện trả lại hoặc hỗ trợ chuyển toàn bộ dữ liệu triển khai và dữ liệu phát sinh trong quá trình sử dụng dịch vụ về cho BIDV;</p> <p>+ Nhà thầu cam kết hoàn thành việc xóa toàn bộ dữ liệu của BIDV ngay khi kết thúc hợp đồng; Đối với các dữ liệu quan trọng hoặc dữ liệu liên quan khách hàng của BIDV phải thực hiện xóa không thể khôi phục lại. Trong trường hợp đặc biệt không thể xóa ngay dữ liệu của BIDV, cần được sự thống nhất của BIDV.</p>
47	<p>Trường hợp hủy dữ liệu: Nhà thầu cam kết hủy dữ liệu khi kết thúc hợp đồng, đảm bảo việc an toàn bảo mật. Hủy toàn bộ các bản backup dữ liệu</p>

48	Nhà thầu đảm bảo phương pháp, giao thức chuyển đổi và định dạng dữ liệu được chuyển đổi phù hợp với tính chất dữ liệu (nếu cần)
<b>VI</b>	<b>Yêu cầu phi chức năng (Hiệu năng, tính năng sẵn sàng, sao lưu, phục hồi, dự phòng, dự phòng thảm họa, khả năng mở rộng)</b>
49	Dịch vụ cloud yêu đáp ứng các yêu cầu hiệu năng như: - Số lượng người sử dụng: tối thiểu 25.000 - Số lượng người sử dụng/kết nối đồng thời: 2.500 - Thời gian xử lý tối đa đối với chức năng/task vụ: 2 giây - Tải hệ thống (load): + Lưu lượng yêu cầu xử lý (request throughput): 1.500 request/giây..
50	- Cam kết mức độ sẵn sàng dịch vụ (SLA) tối thiểu 98% - Thời gian hệ thống ngừng hoạt động tối đa trong một tháng: 2 tiếng
51	Nhà cung cấp đảm bảo yêu cầu về phục hồi: - Thời gian khôi phục dữ liệu (RTO): 0,5 ngày làm việc - Phạm vi phục hồi: + Phục hồi toàn bộ hệ thống (system-level restore) - Yêu cầu về tính toàn vẹn sau phục hồi: dữ liệu, hệ thống, thành phần hệ thống, dịch vụ,... phải được đảm bảo về tính toàn vẹn, đầy đủ, và đảm bảo hoạt động đúng chức năng - Yêu cầu về cơ chế kiểm thử việc khôi phục từ bản sao lưu theo định kỳ (ít nhất 1 lần/năm) và cung cấp báo cáo kết quả kiểm thử cho BIDV. - Yêu cầu về cảnh báo, báo cáo tiến độ và kết quả quá trình phục hồi qua Email
52	Nhà cung cấp đảm bảo yêu cầu về dự phòng thảm họa như sau: - Yêu cầu về RTO (Recovery Time Objective): Thời gian tối đa cho phép để khôi phục dịch vụ sau thảm họa là 1 ngày - Yêu cầu về RPO (Recovery Point Objective): Khoảng thời gian tối đa dữ liệu có thể bị mất: 1 ngày
<b>VII</b>	<b>Yêu cầu về vận hành hệ thống</b>
53	Nhà thầu cung cấp quy trình quản lý thay đổi phiên bản gồm: - Quy trình quản lý thay đổi: backup cấu hình trước thay đổi, phê duyệt khi thay đổi - Thông tin tối thiểu về thay đổi cần quản lý: ai làm, thay đổi gì, thời điểm nào, lý do - Yêu cầu khả năng rollback với các thay đổi. Nhà thầu cung cấp cho BIDV kế hoạch thay đổi phiên bản trước 05 ngày bắt đầu thay đổi qua Email.
54	Nhà thầu cam kết quản trị vận hành cơ sở dữ liệu đáp ứng các yêu cầu: - Thực hiện rà soát, cập nhật các phiên bản vá lỗi hệ điều hành, CSDL tối thiểu 03 tháng một lần (thực hiện rà soát chậm nhất vào tháng giữa quý và hoàn thành đề xuất cập nhật trong quý) và sau khi có khuyến cáo cập nhật lỗi nghiêm trọng của hãng/nhà cung cấp kết hợp với đánh giá mức độ ảnh hưởng của bộ phận quản trị (trong vòng 01 tháng). - Có quy trình/quy định hoặc hướng dẫn được phê duyệt về quản trị, vận hành đối với hệ điều hành và CSDL, trong đó chỉ rõ: + Quy trình kiểm soát an toàn hệ điều hành, CSDL + Phải ghi nhận đầy đủ các sự kiện đối với hệ điều hành và/hoặc CSDL (bao gồm: Nâng cấp/thay đổi phiên bản; Sự cố; Sửa dữ liệu; Thay đổi tham số, cấu hình; Backup, lưu trữ) về thời gian, địa điểm, người thực hiện. - Xây dựng các kế hoạch phản ứng khi xảy ra sự cố đối với CSDL, xác định

	<p>người có trách nhiệm nhận thông tin và xử lý thông tin khi CSDL phát sinh sự cố để có thể kiểm soát, khoanh vùng và giảm thiểu tổn thất, rủi ro phát sinh từ những sự kiện bất ngờ, bao gồm:</p> <ul style="list-style-type: none"> <li>+ Các sự cố phát sinh từ bên ngoài và bên trong hệ CSDL;</li> <li>+ Các sự cố xảy ra trong và ngoài giờ làm việc;</li> <li>+ Các sự cố tác động vào hệ CSDL làm ảnh hưởng đến hoạt động bình thường của CSDL.</li> </ul>
55	<p>Nhà cung thầu cam kết đáp ứng các yêu cầu về ghi log hệ thống, dịch vụ, hoạt động của người dùng như sau:</p> <ul style="list-style-type: none"> <li>- Dữ liệu nhật ký của ứng dụng (logs ứng dụng) phải được bảo vệ, chống truy cập và sửa đổi trái phép bởi người dùng thông thường (chỉ có người quản trị mới có quyền tiếp cận dữ liệu logs của ứng dụng tuy nhiên không thể sửa đổi thông tin)</li> <li>- Trong phạm vi cung cấp dịch vụ cho BIDV, nhà thầu phải đảm bảo lưu trữ online realtime nhật ký (log) sự kiện tối thiểu trong vòng 01 tháng.</li> </ul>
56	<p>Trong trường hợp có sự cố, nhà thầu cam kết thực hiện các yêu cầu sau về quản lý sự cố:</p> <ul style="list-style-type: none"> <li>- Phân loại sự cố theo mức độ ảnh hưởng, tối thiểu bao gồm: <ul style="list-style-type: none"> <li>+ Critical (Nghiêm trọng): Ảnh hưởng toàn hệ thống hoặc dịch vụ trọng yếu ngừng hoạt động.</li> <li>+ High (Lớn): Ảnh hưởng đến một phần lớn người dùng hoặc chức năng chính.</li> <li>+ Low (Nhỏ): Sự cố không ảnh hưởng lớn đến hoạt động chung, có thể khắc phục dễ dàng.</li> </ul> </li> <li>- Cung cấp báo cáo sự cố chi tiết đối với các sự cố mức Critical/Major, bao gồm: <ul style="list-style-type: none"> <li>+ Nguyên nhân gốc rễ (Root Cause Analysis - RCA).</li> <li>+ Tác động của sự cố và các dịch vụ/hệ thống bị ảnh hưởng.</li> <li>+ Thời gian xảy ra và thời gian khắc phục hoàn toàn.</li> <li>+ Biện pháp khắc phục tạm thời và phòng ngừa tái diễn.</li> </ul> </li> <li>- Thời gian cung cấp báo cáo nguyên nhân sự cố: <ul style="list-style-type: none"> <li>• Đối với nghiêm trọng: <ul style="list-style-type: none"> <li>+ Thời gian khắc phục sự cố: &lt; 3h.</li> <li>+ Báo cáo sơ bộ: trong vòng 2 giờ sau khi khắc phục xong sự cố.</li> <li>+ Báo cáo chính thức (RCA đầy đủ): trong vòng 1 - 2 ngày làm việc kể từ thời điểm sự cố kết thúc.</li> </ul> </li> <li>• Đối với sự cố lớn: <ul style="list-style-type: none"> <li>+ Thời gian khắc phục sự cố: &lt; 4h.</li> <li>+ Báo cáo sơ bộ: trong vòng 3-4 giờ sau khi khắc phục xong sự cố.</li> <li>+ Báo cáo chính thức (RCA đầy đủ): trong vòng 3 ngày làm việc kể từ thời điểm sự cố kết thúc.</li> </ul> </li> <li>• Đối với sự cố nhỏ: <ul style="list-style-type: none"> <li>+ Thời gian khắc phục sự cố: &lt; 24h.</li> <li>+ Báo cáo sơ bộ: trong vòng 8 giờ sau khi khắc phục xong sự cố.</li> <li>+ Báo cáo chính thức (RCA đầy đủ): trong vòng 4 ngày làm việc kể từ thời điểm sự cố kết thúc.</li> <li>• Thời gian khắc phục sự cố tính từ lúc nhà thầu nhận được thông tin từ BIDV.</li> </ul> </li> </ul> </li> </ul>

	<ul style="list-style-type: none"> <li>- Cung cấp cơ chế thông báo sự cố theo thời gian thực (real-time), thông qua các kênh như email, SMS, webhook, dashboard monitoring hoặc API tích hợp.</li> <li>- Cung cấp tài liệu hỗ trợ xử lý sự cố, bao gồm: <ul style="list-style-type: none"> <li>+ Hướng dẫn vận hành (runbook) nếu cần;</li> <li>+ Kịch bản xử lý tình huống (incident playbook).</li> </ul> </li> <li>- Hỗ trợ truy vết và kiểm tra nhật ký sự cố, phục vụ cho việc điều tra và kiểm toán sau này.</li> </ul>
57	<p>Nhà thầu cam kết thực hiện báo cáo và đánh giá định kỳ và gửi cho BIDV về:</p> <ul style="list-style-type: none"> <li>- Tình trạng hoạt động của dịch vụ (trạng thái hệ thống, uptime, downtime, lỗi sự cố,...)</li> <li>- Các rủi ro/vấn đề tồn tại và đề xuất hướng xử lý.</li> </ul>
<b>VIII</b>	<b>Yêu cầu khi kết thúc sử dụng dịch vụ</b>
58	<p>Cam kết trả lại và chuyển giao dữ liệu:</p> <ul style="list-style-type: none"> <li>- Đảm bảo yêu cầu xuất toàn bộ dữ liệu của BIDV dưới định dạng chuẩn, có thể đọc và sử dụng được bởi hệ thống khác.</li> <li>- Quá trình chuyển giao phải bảo đảm toàn vẹn, đầy đủ, không mất mát dữ liệu.</li> <li>- Nhà cung cấp cần phối hợp hỗ trợ chuyển dữ liệu sang hệ thống mới nếu BIDV yêu cầu</li> </ul>
59	<p>Cam kết xóa dữ liệu:</p> <ul style="list-style-type: none"> <li>- Sau khi BIDV xác nhận đã nhận đủ dữ liệu, nhà cung cấp phải xóa toàn bộ bản sao dữ liệu còn lại trên hạ tầng của mình, trừ khi có yêu cầu lưu trữ khác theo luật định.</li> <li>- Quá trình xóa phải được thực hiện theo chuẩn bảo mật quốc tế (trung tự như NIST 800-88) và có biên bản xác nhận gửi BIDV.</li> </ul>
60	<p>Cam kết ngừng truy cập và thu hồi quyền:</p> <ul style="list-style-type: none"> <li>- Ngay khi kết thúc hợp đồng, nhà cung cấp phải thu hồi toàn bộ quyền truy cập của người dùng và hệ thống liên quan đến BIDV.</li> <li>- Các thông tin xác thực, mã truy cập, tài khoản quản trị phải được vô hiệu hóa hoặc chuyển giao theo yêu cầu của BIDV.</li> </ul>
61	<p>Cam kết thời gian hỗ trợ kỹ thuật trong một khoảng thời gian tối thiểu 5 ngày sau khi kết thúc thời gian sử dụng dịch vụ, nhằm hỗ trợ xử lý sự cố phát sinh trong quá trình thoát khỏi.</p>
62	<ul style="list-style-type: none"> <li>- Trường hợp nhà cung cấp không đáp ứng yêu cầu bảo mật, xảy ra sự cố nghiêm trọng, hoặc có rủi ro ảnh hưởng đến hoạt động, BIDV có quyền yêu cầu thoát khỏi nhà cung cấp ngay lập tức và phạt vi phạm, cấm tham gia các gói thầu của BIDV.</li> </ul>
63	<p>Yêu cầu khác: Nhà cung cấp Cloud, Nhà thầu cung cấp cam kết bảo mật thông tin của BIDV</p>
<b>X</b>	<b>Yêu cầu dịch vụ hỗ trợ</b>
64	<p>Nhà thầu chịu trách nhiệm vận hành và hỗ trợ kỹ thuật</p>
65	<p>Nhà thầu đáp ứng việc hỗ trợ các yêu cầu của BIDV qua Email. Thời gian phản hồi/xử lý với các sự cố thực hiện theo yêu cầu tại mục 49, với các hỗ trợ khác như sau:</p> <ul style="list-style-type: none"> <li>- Với các yêu cầu không cần thực hiện gấp: Trong vòng 24h theo ngày làm việc, tính từ khi nhận được thông tin từ BIDV.</li> <li>- Với các yêu cầu gấp: Trong vòng 30 phút sau khi nhận được yêu cầu hỗ trợ,</li> </ul>

	tính từ khi nhận được thông tin từ BIDV.
<b>XI</b>	<b>Yêu cầu về đào tạo</b>
66	<p>Nhà thầu cung cấp dịch vụ đào tạo liên quan đến triển khai hệ thống, nhân sự đào tạo có thể là chính hãng hoặc nhân sự của nhà thầu có đủ năng lực và kinh nghiệm thực hiện như sau:</p> <ul style="list-style-type: none"> <li>- Thời gian thực hiện đào tạo: Trong khoảng thời gian triển khai dự án;</li> <li>- Địa điểm đào tạo: Tại BIDV hoặc đào tạo online</li> <li>- Hình thức đào tạo: Trực tiếp/online</li> <li>- Nội dung đào tạo: <ul style="list-style-type: none"> <li>+ Đào tạo quản trị vận hành hệ thống</li> <li>+ Đào tạo cán bộ làm công tác đào tạo</li> <li>+ Đào tạo giảng viên (nếu cần)</li> <li>+ Đào tạo học viên sử dụng</li> </ul> </li> <li>- Số khóa đào tạo: tối thiểu 4</li> <li>- Tài liệu đào tạo: Ngôn ngữ tiếng Việt</li> <li>- Đối tượng đào tạo: Cán bộ quản trị vận hành, cán bộ làm công tác đào tạo, giảng viên, đầu mối đào tạo các đơn vị và học viên thuộc các đơn vị</li> </ul>
<b>XII</b>	<b>Yêu cầu về chuyển giao</b>
67	<p>Tài liệu bàn giao:</p> <ul style="list-style-type: none"> <li>- Các tài liệu tối thiểu theo các hạng mục của dự án: Tài phân tích khác biệt (gap); Tài liệu quản trị vận hành; Tài liệu đào tạo;...</li> <li>- Tài liệu về hệ thống/dịch vụ: Tài liệu kỹ thuật, Hướng dẫn sử dụng dịch vụ, Quy trình tiếp nhận và xử lý sự cố/hỗ trợ kỹ thuật, Quy trình sao lưu/phục hồi dữ liệu phù hợp với dịch vụ cung cấp cho BIDV và đảm bảo BIDV có thể giám sát, theo dõi chất lượng dịch vụ.</li> </ul>
68	Sản phẩm bàn giao: Quyền sử dụng hệ thống quản lý đào tạo