Phần 2. YÊU CẦU VỀ KỸ THUẬT
Chương V. YÊU CẦU VỀ KỸ THUẬT

Mục 1. Yêu cầu về kỹ thuật

1.1. Giới thiệu chung về dự án/dự toán mua sắm, gói thầu

*** Tên dự toán mua sắm:** Thay thế thiết bị tường lửa và triển khai hệ thống mạng WAN của KTNN.

*** Tên gói thầu:** Thay thế thiết bị tường lửa và triển khai hệ thống mạng WAN của KTNN Kiểm toán nhà nước.

*** Địa điểm thực hiện:** Trụ sở của Kiểm toán nhà nước tại 116 Nguyễn Chánh, Hà Nội; 111 Trần Duy Hưng, Hà Nội và các Kiểm toán nhà nước khu vực

*** Mục tiêu mua sắm:**

Thay thế thiết bị tường lửa và triển khai hệ thống mạng WAN của KTNN Kiểm toán nhà nước nhằm đảm bảo đáp ứng được yêu cầu về an ninh bảo mật, độ ổn định của kết nối, chất lượng của kết nối cũng như khả năng quản lý tập trung của mạng WAN phục vụ hoạt động của KTNN.

Việc đầu tư hệ thống SD-WAN nhằm giải quyết các tồn tại, hạn chế trong mô hình kết nối mạng hiện tại của các Kiểm toán nhà nước (KTNN) khu vực và đảm bảo đáp ứng yêu cầu ngày càng cao về hiệu năng, bảo mật và quản lý tập trung trong bối cảnh phát triển hạ tầng CNTT của KTNN:

Cung cấp hệ thống quản trị tập trung giúp quản trị, giám sát và cấu hình tập trung các thiết bị WAN tại Trung tâm dữ liệu 116 Nguyễn Chánh và Trung tâm dữ liệu 111 Trần Duy Hưng, các KTNN khu vực.

Đảm bảo chất lượng dịch vụ và chất lượng đường truyền WAN, QoS cho các dịch vụ

Đảm bảo cung cấp khả năng dự phòng, cân bằng tải giữa các đường truyền WAN linh hoạt, có khả năng chuyển đổi nhanh chóng, tránh độ trễ kết nối.

Cung cấp khả năng phân tách các loại lưu lượng như: Lưu lượng người dùng ra internet tại đơn vị, lưu lượng kết nối về các hệ thống tại Trung tâm dữ liệu 116 Nguyễn Chánh và Trung tâm dữ liệu 111 Trần Duy Hưng, các KTNN khu vực.

*** Quy mô của dự toán mua sắm:**

TT	Tên thiết bị	Vị trí	Đơn vị tính	Số lượng
1	Hệ thống quản trị tập trung SDWAN	DC	Bộ	1
2	Thiết bị SD-WAN tại DC	DC	Chiếc	2
3	Thiết bị SDWAN tại kiểm toán khu vực	KTNN Khu vực	Chiếc	26

*** Yêu cầu chi tiết về cung cấp hàng hóa của gói thầu:** Chi tiết tại Mục 1.2 Chương V E-HSMT

*** Thời gian thực hiện gói thầu:** 90 ngày.

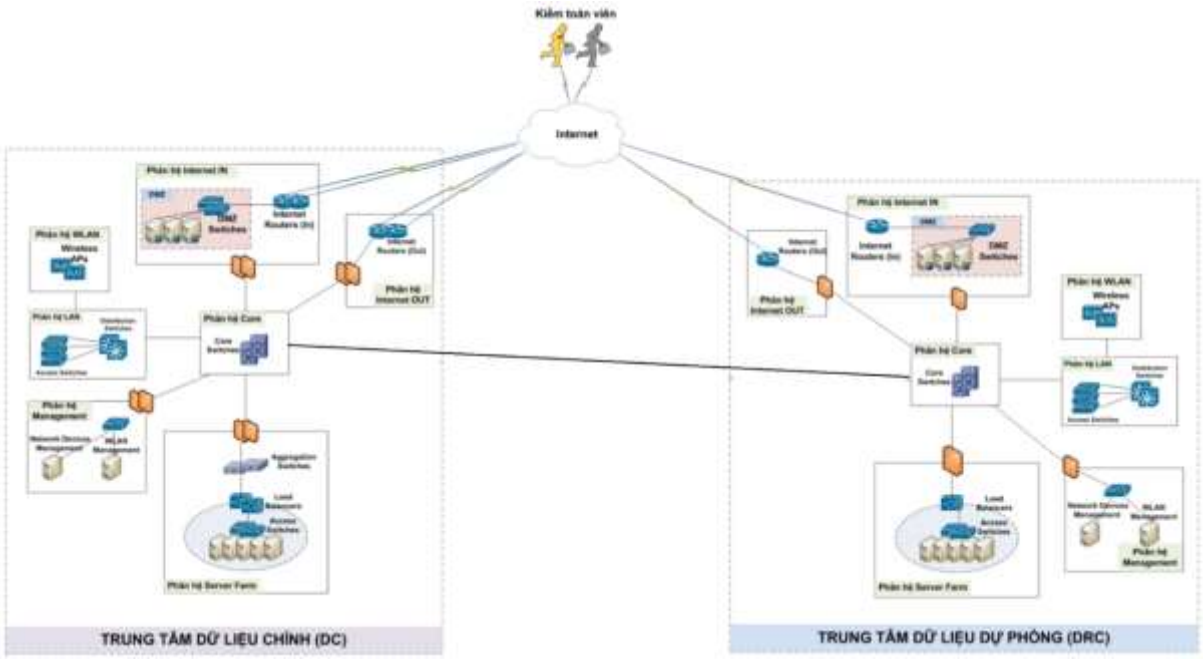
*** Giới thiệu về hiện trang cơ sở hạ tầng và ứng dụng công nghệ thông tin:**

*****Về hạ tầng kỹ thuật - CNTT của KTNN:***

Hiện trạng đầu tư hệ thống công nghệ thông tin (CNTT):

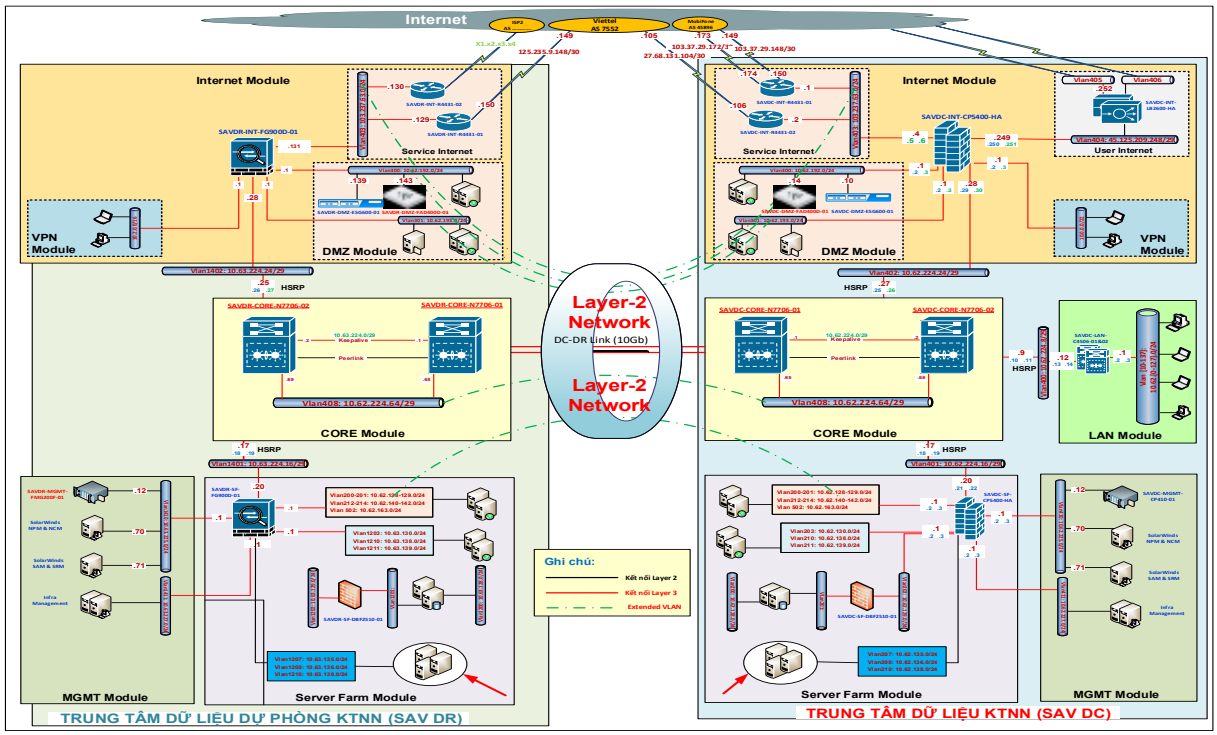
Hiện nay, hạ tầng CNTT của KTNN đã được đầu tư, trang bị máy móc thiết bị sử dụng các công nghệ tiên tiến, có khả năng đáp ứng yêu cầu cho việc triển khai các phần mềm ứng dụng và dịch vụ mạng hiện có của KTNN. KTNN đã xây dựng Trung tâm dữ liệu (TTDL) chính tại 116 Nguyễn Chánh, Hà Nội. Các máy chủ tại TTDL có đầy đủ bản quyền hệ điều hành Windows Server và hệ quản trị cơ sở dữ liệu MS SQL, Thiết bị an ninh bảo mật có đầy đủ bản quyền cập nhật các mẫu tấn công của các hãng bảo mật… TTDL đã cơ bản đáp ứng tiêu chuẩn đối với TTDL theo quy định của Bộ Thông tin và Truyền thông tại Thông tư số 03/2013/TT-BTTTT ngày 22/01/2013. Trong năm 2019, KTNN xây dựng TTDL dự phòng tại Trụ sở 111 Trần Duy Hưng, hình thành hạ tầng CNTT thống nhất để lưu trữ tập trung, đảm bảo tính dự phòng cao, hoạt động ổn định và liên tục của hệ thống thông tin KTNN.

a) Mô hình tổng thể hệ thống CNTT



Mô hình tổng thể hệ thống CNTT của KTNN

b) Mô hình kết nối vật lý hệ thống CNTT



Mô hình kết nối vật lý hệ thống CNTT của KTNN

Hạ tầng CNTT của KTNN đã được đầu tư theo từng giai đoạn phù hợp với yêu cầu phát triển các phần mềm ứng dụng, cơ sở dữ liệu và các dịch vụ mạng của KTNN. Trong thời gian tới, khi KTNN tiếp tục triển khai các phần mềm, cơ sở dữ liệu cần phải tiếp tục đầu tư hạ tầng kỹ thuật cho phù hợp. Theo đánh giá

sơ bộ, hạ tầng hiện nay có thể đáp ứng yêu cầu hạ tầng kỹ thuật cho Cơ sở dữ liệu dùng chung hoạt động.

Hiện trạng hệ thống an ninh bảo mật:

a) Hiện trạng hạ tầng mạng và bảo mật

Hạ tầng mạng và bảo mật thuộc TTDL của KTNN sau các giai đoạn đầu tư đã tương đối đầy đủ các thành phần cần thiết, đáp ứng cơ bản yêu cầu đối với hệ thống thông tin cấp độ 3 (Theo phụ lục 3 Ban hành kèm theo Thông tư số 03/2017/TT-BTTTT ngày 24 tháng 4 năm 2017 của Bộ trưởng Bộ Thông tin và Truyền thông):

Yêu cầu thuộc TT 03 đáp ứng các yêu cầu đảm bảo ATTT cho các hệ thống thông tin cấp độ 3	Hiện trạng KTNN (Phân vùng TTDL)
Yêu cầu về kỹ thuật	
a) An toàn hạ tầng mạng	
Có thiết kế vùng mạng dành riêng bao gồm vùng mạng riêng cho máy chủ nội bộ, vùng mạng riêng cho các máy chủ cung cấp các dịch vụ hệ thống cần thiết (như dịch vụ DNS, DHCP, NTP và các dịch vụ khác), vùng mạng riêng cho máy chủ cơ sở dữ liệu và các vùng mạng riêng khác theo yêu cầu của tổ chức	Có (theo hiện trạng mô hình logic)
Có thiết kế vùng mạng nội bộ thành các mạng chức năng riêng theo yêu cầu nghiệp vụ; phân vùng mạng riêng cho mạng không dây tách biệt với các vùng mạng chức năng; phân vùng mạng riêng cho các máy chủ cung cấp dịch vụ ra ngoài mạng Internet	Có
Có phương án cân bằng tải và giảm thiểu tấn công từ chối dịch vụ	Có (F5, IPS TrendMicro vùng DMZ; A10 vùng User Internet)
Có thiết kế hệ thống quản lý lưu trữ tập trung và giám sát an toàn thông tin	Có (Splunk)
Có phương án sử dụng thiết bị có chức năng tường lửa giữa các vùng mạng quan trọng	Có (Firewall CP, Paloalto vùng DC; FW Fortigate vùng DR)
Có phương án phát hiện, phòng chống xâm nhập và	Có (IPS TrendMicro)

chặn lọc phần mềm độc hại giữa mạng Internet và các mạng bên trong	
Có lưu trữ nhật ký các thiết bị mạng và quản lý tập trung trong vùng mạng quản trị đối với các thiết bị mạng có hỗ trợ tính năng này hoặc thiết bị mạng quan trọng	Có
Có lưu trữ tối thiểu trong 03 tháng đối với nhật ký của các thiết bị mạng và bảo đảm đồng bộ thời gian nhật ký với máy chủ thời gian thực theo múi giờ Việt Nam	Có
Có thiết kế dự phòng cho các thiết bị mạng chính trong hệ thống bảo đảm duy trì hoạt động bình thường của hệ thống khi một thiết bị mạng gặp sự cố	Tại DC: Có Tại DR: Chưa đảm bảo
Có phương án cập nhật phần mềm, xử lý điểm yếu an toàn thông tin và cấu hình tối ưu thiết bị mạng trước khi đưa vào sử dụng trong mạng	Có
Có phương án xác thực tài khoản quản trị trên tất cả các thiết bị mạng trong đó bảo đảm yêu cầu về mật khẩu có độ phức tạp cần thiết, phòng chống dò quét mật khẩu	Có (PIM CyberArk)
Có phương án giới hạn các nguồn truy cập, quản trị các thiết bị mạng	Có
Có phương án chỉ cho phép quản trị các thiết bị mạng thông qua mạng Internet bằng mạng riêng ảo hoặc các phương pháp khác tương đương	Có
Có ghi nhật ký đối với các hoạt động trên thiết bị mạng nội bộ và bảo đảm đồng bộ thời gian nhật ký với máy chủ thời gian	Có
Có mã hóa thông tin xác thực lưu trên thiết bị mạng	Có
b) An toàn máy chủ	
Có phương án quản lý xác thực tập trung; chống đăng nhập tự động và tự động hủy phiên đăng nhập sau một khoảng thời gian chờ phù hợp với chính	Có giải pháp

sách của tổ chức	
Có thiết lập quyền truy cập, quản trị, sử dụng tài nguyên của từng tài khoản trên hệ thống phù hợp với nhiệm vụ, yêu cầu nghiệp vụ khác nhau	Có giải pháp
Có phương án quản lý bản vá, nâng cấp phần mềm hệ thống tập trung	Có giải pháp
Có phương án lưu trữ và quản lý tập trung nhật ký máy chủ. Nhật ký được lưu tối thiểu 03 tháng	Có giải pháp
Có phương án đồng bộ nhật ký máy chủ với hệ thống giám sát an toàn thông tin	Có giải pháp
Có phương án giới hạn các nguồn cho phép truy cập, quản trị máy chủ; việc quản trị máy chủ thông qua mạng Internet phải sử dụng mạng riêng ảo hoặc các phương pháp khác tương đương	Có
Có phương án sử dụng tường lửa trên từng máy chủ nhằm thiết lập chỉ cho phép các kết nối hợp pháp theo các dịch vụ được máy chủ cung cấp	Có giải pháp
Có phương án sao lưu dự phòng hệ điều hành máy chủ, cấu hình máy chủ phù hợp với yêu cầu của tổ chức	Có
Có ghi nhật ký đối với các hoạt động truy cập, quản trị, phát sinh lỗi	Có
c) An toàn ứng dụng	
Có thiết lập yêu cầu thay đổi mật khẩu định kỳ đối với tài khoản quản trị ứng dụng; giới hạn thời gian chờ để đóng phiên kết nối khi ứng dụng không nhận được yêu cầu từ người dùng	Có
Có thiết lập tách biệt ứng dụng quản trị với ứng dụng cung cấp dịch vụ cho người sử dụng và bảo đảm ứng dụng hoạt động với quyền tối thiểu trên hệ thống	Có
Có phương án giới hạn các nguồn cho phép truy cập, quản trị ứng dụng; việc quản trị ứng dụng thông qua mạng Internet phải sử dụng mạng riêng ảo hoặc các	Có

phương pháp khác tương đương	
Có phương án kiểm tra, lọc các dữ liệu đầu vào từ phía người sử dụng, bảo đảm các dữ liệu này không ảnh hưởng đến an toàn thông tin của ứng dụng	Có
d) An toàn dữ liệu	
Có phương án mã hóa dữ liệu lưu trữ (không phải là thông tin, dữ liệu công khai) trên hệ thống lưu trữ/phương tiện lưu trữ	Có giải pháp
Có phương án tự động sao lưu dự phòng đối với thông tin/dữ liệu phù hợp với tần suất thay đổi của dữ liệu	Có giải pháp
Yêu cầu về quản lý	
a) Chính sách chung: Định kỳ 02 năm hoặc đột xuất khi cần thiết thực hiện rà soát, cập nhật chính sách chung về an toàn thông tin;	Có
b) Tổ chức, nhân sự:	
- Có kế hoạch và định kỳ tổ chức đào tạo, bồi dưỡng, tuyên truyền, phổ biến nâng cao kiến thức, kỹ năng về an toàn thông tin cho cán bộ quản lý và cán bộ kỹ thuật có liên quan	Có
- Có chính sách yêu cầu cán bộ liên quan khi thôi việc cần cam kết giữ bí mật thông tin liên quan đến dữ liệu trên hệ thống, thông tin riêng của tổ chức hoặc thông tin nhạy cảm khác	Có
c) Thiết kế, xây dựng hệ thống:	
Có hồ sơ đề xuất cấp độ được thẩm định bởi đơn vị chuyên trách về an toàn thông tin của chủ quản hệ thống thông tin	Có
d) Quản lý vận hành:	
- Có phương án giám sát an toàn thông tin cho hệ thống trong quá trình vận hành theo quy định của pháp luật	Có

- Có kế hoạch và định kỳ tổ chức diễn tập bảo đảm an toàn thông tin cho hệ thống; cử cán bộ tham gia vào các cuộc diễn tập quốc gia hoặc quốc tế do cơ quan chức năng triệu tập	Có
- Có kế hoạch khôi phục hoạt động bình thường của hệ thống trong trường hợp xảy ra sự cố hoặc thảm họa	Có
đ) Kiểm tra, đánh giá và quản lý rủi ro:	
- Định kỳ hàng năm thực hiện kiểm tra, đánh giá an toàn thông tin và quản lý rủi ro an toàn thông tin theo quy định của pháp luật	Có
- Việc kiểm tra, đánh giá an toàn thông tin và đánh giá rủi ro phải do tổ chức chuyên môn được cơ quan có thẩm quyền cấp phép hoặc tổ chức sự nghiệp nhà nước có chức năng, nhiệm vụ phù hợp do chủ quản hệ thống thông tin chỉ định thực hiện theo quy định của pháp luật.	Có

b) Hiện trạng hạ tầng mạng LAN/WAN

Hạ tầng mạng LAN (người dùng) hiện tại ở KTNN đáp ứng cơ bản các tiêu chí như sau:

Yêu cầu về thiết kế hệ thống đảm bảo an toàn (theo TCVN 11930:2017 dành cho hệ thống thông tin cấp độ 3)	Hiện trạng KTNN (phân vùng mạng người dùng)
Có phương án quản lý truy cập, quản trị hệ thống từ xa an toàn	Có (hệ thống VPN - FW Paloalto)
Có phương án quản lý truy cập giữa các vùng mạng và phòng chống xâm nhập	Có (Firewall Paloalto, Checkpoint)
Có phương án cân bằng tải và dự phòng nóng cho các thiết bị mạng chính	Có (các thiết bị mạng chính đều chạy theo cặp, chia tải và dự phòng)
Có phương án bảo đảm an toàn cho máy chủ CSDL	Có (Database Security - Imperva)
Có phương án giám sát lưu lượng mạng	Chưa có giải pháp giảm sát lưu

	lượng mạng ở các phân đoạn mạng quan trọng
Có phương án phòng chống tấn công từ chối dịch vụ	Có (IPS TrendMicro)
Có phương án giám sát hệ thống thông tin tập trung	Có (SIEM Splunk)
Có phương án giám sát an toàn hệ thống thông tin tập trung	
Có phương án quản lý sao lưu dự phòng tập trung	Có (Dell EMC Networker)
Có phương án quản lý phần mềm phòng chống mã độc trên các máy chủ/máy tính người dùng tập trung	Có (Trendmicro) Chưa có giải pháp phát hiện và phản hồi các mối nguy hại cho lớp máy trạm
Có phương án phòng, chống thất thoát dữ liệu	Chưa có
Có phương án dự phòng kết nối mạng Internet cho các máy chủ dịch vụ	Có
Có phương án giải pháp quản trị, giám sát, bảo mật truy cập Web cho người dùng	Chưa có

Hạ tầng mạng WAN hiện tại của KTNN về cơ bản là các kết nối VPN Site to Site từ DC, DR tới 13 khu vực qua các kênh truyền Internet.

c) Cấp độ an toàn thông tin được phê duyệt

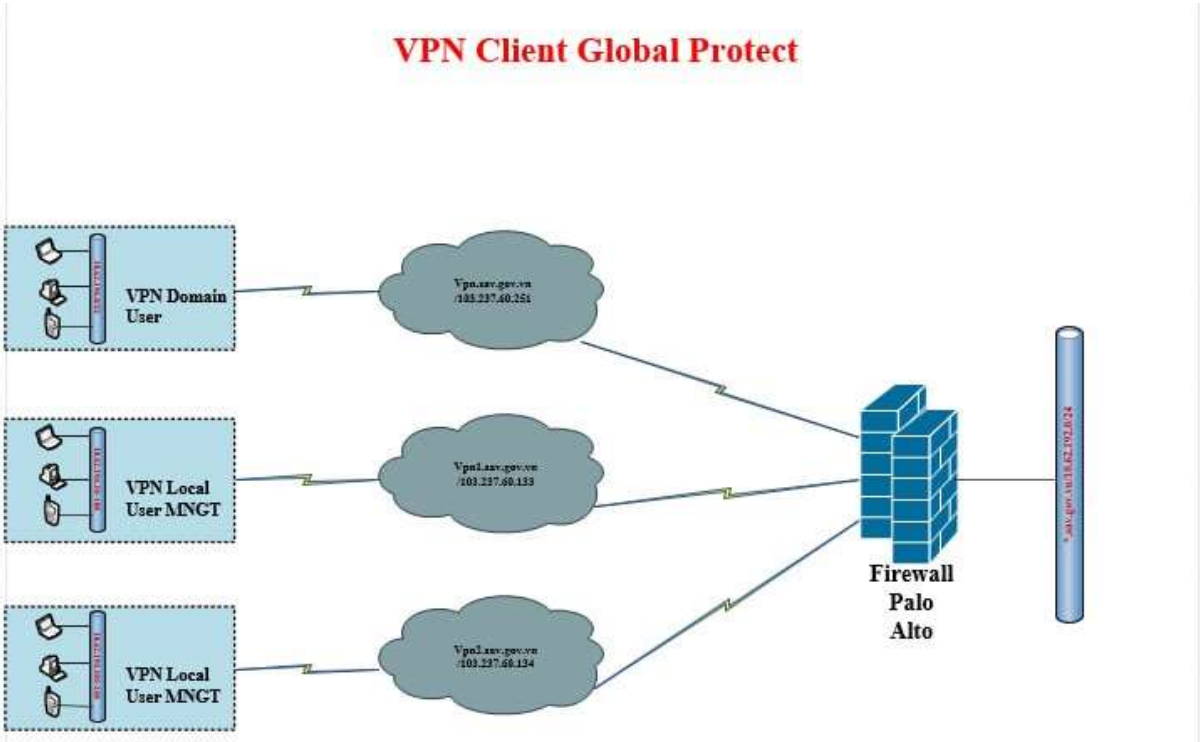
Tại Quyết định số 1948/QĐ-KTNN ngày 24/11/2021, Tổng Kiểm toán nhà nước đã phê duyệt cấp độ an toàn hệ thống thông tin Kiểm toán nhà nước là cấp độ 3. Đơn vị vận hành hệ thống thông tin là Cục Công nghệ thông tin đã triển khai các phương án bảo đảm an toàn thông tin trong thiết kế và vận hành hệ thống tương ứng với cấp độ 3 tuân thủ theo tiêu chuẩn quốc gia TCVN 11930:2017.

d) Hiện trạng kết nối VPN đối với phần mềm nội bộ của KTNN

Để tăng cường tính bảo mật cho hệ thống mạng và ứng dụng của Kiểm toán nhà nước, người dùng cần sử dụng VPN để kết nối đến mạng nội bộ của Kiểm toán nhà nước. VPN của Kiểm toán nhà nước sử dụng phần mềm Global Protect của hãng Palo Alto, phần mềm có thể cài đặt được trên các thiết bị máy tính

Windows, Mac, các thiết bị di động thông minh có hệ điều hành của IOS và Android.

Mô hình mạng kết nối



- Đối với người dùng là cán bộ công nhân viên của Kiểm toán nhà nước

+ Cài đặt phần mềm Global Protect trên thiết bị sử dụng (đã có hướng dẫn sử dụng phù hợp với thiết bị).

+ Có sử dụng Internet và kết nối VPN đến domain của kiểm toán nhà nước.

+ Sử dụng tài khoản của cán bộ được cấp truy cập vào ứng dụng để đăng nhập vào ứng dụng Global Protect.

+ Sau khi kết nối VPN, cán bộ kiểm toán có thể truy cập được vào các trang nội bộ của kiểm toán nhà nước

- Đối với người dùng là cán bộ công nhân viên của Kiểm toán nhà nước thuộc phòng hệ thống CNTT hoặc cán bộ hỗ trợ quản trị hệ thống cho Kiểm toán nhà nước

+ Cài đặt phần mềm Global Protect trên thiết bị sử dụng (đã có hướng dẫn sử dụng phù hợp với thiết bị)

+ Có sử dụng Internet và kết nối VPN đến domain của kiểm toán nhà nước.

+ Sử dụng tài khoản của cán bộ được cấp truy cập vào ứng dụng để kết nối hoặc tài khoản được tạo trên thiết bị của hãng Palo Alto để đăng nhập

vào ứng dụng Global Protect.

+ Sau khi kết nối VPN, cán bộ kiểm toán có thể truy cập được vào các trang nội bộ của kiểm toán, kết nối vào các trang quản trị thiết bị hệ thống qua phần mềm Cyberark được cung cấp cho các cán bộ nhân viên.

- Đối với người dùng là cán bộ công nhân viên của Kiểm toán nhà nước thuộc phòng phần mềm CNTT hoặc cán bộ hỗ trợ ứng dụng cho Kiểm toán nhà nước:

+ Cài đặt phần mềm Global Protect trên thiết bị sử dụng (đã có hướng dẫn sử dụng phù hợp với thiết bị)

+ Có sử dụng Internet và kết nối VPN đến domain của kiểm toán nhà nước.

+ Sử dụng tài khoản của cán bộ được cấp truy cập vào ứng dụng để kết nối hoặc tài khoản được tạo trên thiết bị của hãng Palo Alto để đăng nhập vào ứng dụng Global Protect.

+ Sau khi kết nối VPN, cán bộ kiểm toán có thể truy cập được vào các trang nội bộ của kiểm toán, kết nối vào các trang quản trị thiết bị hệ thống qua phần mềm Cyberark được cung cấp cho các cán bộ nhân viên.

****Hiện trạng hệ thống tường lửa tại các Kiểm toán nhà nước khu vực và kết nối mạng giữa các đơn vị của Kiểm toán nhà nước:**

Các thiết bị tường lửa tại các KTNN Khu vực đang sử dụng thiết bị Check Point 3100 Security Gateway được đầu tư theo Hợp đồng số 26/2017/HĐKT/HIPT-BQLCNTT ngày 26/9/2017 giữa Ban Quản lý dự án công nghệ thông tin thuộc Kiểm toán nhà nước với công ty cổ phần tập đoàn HIPT. Thiết bị hết thời hạn bảo hành vào tháng 12/2024. Thiết bị đã được sử dụng trên 07 năm và sẽ hết hạn hỗ trợ của hãng (end of suport) vào tháng 12/2025.

Các thiết bị tường lửa tại 13 KTNN Khu vực hiện nay có chức năng kết nối mạng WAN với TTDL của KTNN qua kết nối VPN Site to Site. Về cơ bản, phương án kết nối này đã tạo thành 1 mạng WAN tuy nhiên đang tồn tại một số điểm hạn chế sau:

+ Không có cơ chế quản lý toàn bộ các thiết bị thuộc mạng WAN

+ Không thực hiện được tính năng ưu tiên dịch vụ (QoS), các ứng dụng và dịch vụ yêu cầu độ trễ thấp như VoIP và hội nghị truyền hình sẽ không đạt được chất lượng dịch vụ như mong muốn.

+ Không có cơ chế gộp đường truyền để tăng băng thông, chia tải dẫn tới khi 1 đường truyền gặp sự cố thì gây gián đoạn tới kết nối.

+ Không phân tách giữa lưu lượng mạng người dùng truy cập internet với lưu lượng mạng giữa các site, điều này có thể gây mất an toàn an ninh bảo mật hệ thống của KTNN.

+ Việc kết nối thường xảy ra các vấn đề như: Kết nối không ổn định, hay xảy ra gián đoạn; Mất cấu hình kết nối, cần cấu hình lại thiết bị để kết nối VPN, tốc độ kết nối chậm, ...

Các thiết bị tường lửa tại các KTNN khu vực đang sử dụng cấu hình thấp không bật được nhiều tính năng bảo mật nâng cao và lạc hậu về công nghệ nên khó tích hợp với các giải pháp công nghệ bảo mật mới hiện nay.

Ngoài ra, thiết bị tường lửa internet của Trung tâm dữ liệu chính DC khác với thiết bị tường lửa tại Trung tâm dữ liệu dự phòng DR (DC sử dụng thiết bị paloalto, DR sử dụng thiết bị Fortigate). Do vậy, mạng WAN hiện tại chỉ kết nối giữa các khu vực với DC, chưa kết nối với DR, do vậy chưa đảm bảo dự phòng.

1.2. Yêu cầu về kỹ thuật

1.2.1. Yêu cầu kỹ thuật chung:

- Tiêu chuẩn hàng hóa:

+ Các sản phẩm nhà thầu cung cấp phải mới 100%, sản xuất từ năm 2024 trở lại đây, đã bao gồm đầy đủ các vật tư, phụ kiện và dịch vụ kỹ thuật kèm theo để lắp đặt hoàn chỉnh, vận hành theo yêu cầu của chủ đầu tư. Hàng hóa phải có nguồn gốc, xuất xứ rõ ràng, đúng chủng loại, đảm bảo chất lượng theo yêu cầu của Chủ đầu tư.

+ Đối với hàng hoá nhập khẩu: Cam kết cung cấp Giấy chứng nhận chất lượng của nhà sản xuất (C/Q) và Giấy chứng nhận chất lượng xuất xứ (C/O) khi bàn giao hàng hoá.

+ Đối với hàng hoá sản xuất trong nước: Cam kết cung cấp Giấy chứng nhận chất lượng của nhà sản xuất (C/Q) hoặc phiếu xuất xưởng khi bàn giao hàng hoá.

+ Đối với phần mềm: Cam kết phần mềm không vi phạm bản quyền và chịu trách nhiệm về mọi thiệt hại phát sinh do việc khiếu nại của bên thứ ba về vi phạm bản quyền sở hữu trí tuệ liên quan tới phần mềm mà nhà thầu đã cung cấp.

- Tài liệu chứng minh sự phù hợp của hàng hóa:

Nhà thầu nộp tài liệu kỹ thuật (catalogue, hướng dẫn sử dụng ,…) của nhà sản xuất (hãng sản xuất) chứng minh hàng hóa dự thầu đáp ứng yêu cầu kỹ thuật của E-HSMT. Trường hợp các tài liệu này bằng tiếng nước ngoài thì phải đính kèm bản dịch tiếng Việt và nhà thầu chịu trách nhiệm về tính chính xác nội dung bản dịch. Bản dịch tiếng Việt có thể dịch toàn bộ tài liệu hoặc tóm tắt nội dung nhưng phải chứng minh được hàng hoá đáp ứng đầy đủ các yêu cầu tại Chương V của E-HSMT.

1.2.2. Yêu cầu kỹ thuật chi tiết:

Hàng hóa, dịch vụ liên quan phải tuân thủ các thông số kỹ thuật và tiêu chuẩn sau đây:

TT	Tên thiết bị	Vị trí	Đơn vị tính	Số lượng
1	**Hệ thống quản trị tập trung SDWAN**	**DC**	**Bộ**	**1**
	Được triển khải ở dạng ảo hóa được cài đặt trên hệ thống máy chủ tại DC/DR Quản lý được các thiết bị SDWAN trong mạng Có tính năng SD-WAN monitoring, cho phép giám sát lịch sử chất lượng đường truyền với các thông số Jitter, Packet Loss và Latency. Hỗ trợ quản lý tối thiểu cho 40 thiết bị và có khả năng mở rộng. Bảo hành chính hãng 03 năm Bản quyền, hỗ trợ kỹ thuật 3 năm			
2	**Thiết bị SD-WAN tại DC**	DC	**Chiếc**	**2**
	Có khả năng tích hợp được với thiết bị SDWAN tại DR (Fortigate 900D) Hỗ trợ SSLVPN tối thiểu 2.000 user IPSEC throughtput 55 Gbps Firewall throughput 130 Gbps NGFW 22 Gbps Threat Prevention throughput 10.5 Gbps Bảo hành chính hãng 03 năm Hỗ trợ kỹ thuật chính hãng 03 năm			
3	**Thiết bị SDWAN tại kiểm toán khu vực**	**KTNN Khu vực**	**Chiếc**	**26**

	Có khả năng tích hợp được với thiết bị SDWAN tại DR (Fortigate 900D) IPSEC Throughput: 6.5 Gbps NGFW 1 Gbps Thread Prevention throughput 900Mbps Bảo hành chính hãng 3 năm Hỗ trợ kỹ thuật chính hãng 3 năm			

Yêu cầu kỹ thuật chi tiết:

STT	Yêu cầu kỹ thuật	Thông số kỹ thuật
I	**Yêu cầu về phần cứng cho thiết bị tại các KTNN Khu vực**	
1.1	Số lượng giao diện mạng	Tối thiểu 6 cổng 1GE RJ45 Tối thiểu 2 cổng WAN 1GE RJ45
1.2	Thông lượng Firewall	≥ 10 Gbps
1.3	Thông lượng IPsec VPN	≥ 6.5 Gbps
1.4	Thông lượng IPS (Trong môi trường thực tế)	≥ 1.4 Gbps
1.5	Thông lượng NGFW (Trong môi trường thực tế)	≥ 1 Gbps
1.6	Thông lượng Threat Protection (Trong môi trường thực tế)	≥ 900 Mbps
1.7	Số lượng kết nối đồng thời (Concurrent Sessions)	≥ 1.5 Million
1.8	Số kết nối mới/giây (New Sessions/Second)	≥ 45.000
1.9	Số lượng Firewall ảo có sẵn	≥ 10

STT	Yêu cầu kỹ thuật	Thông số kỹ thuật
1.10	Hỗ trợ tính năng IPS	Hỗ trợ phát hiện giao thức bất thường, ngưỡng bất thường, tự định nghĩa signature.
1.11	Hỗ trợ tính năng Anti-Virus/ Malware, URL Filtering	Antivirus và phòng chống Botnet, Content disarm and reconstruction (CDR) Hỗ trợ tính năng URL Filtering
1.12	Chế độ dự phòng	Hỗ trợ Active-Active, Active-Passive, Clustering
1.13	Bảo hành và hỗ trợ kỹ thuật	3 năm bảo hành và hỗ trợ kỹ thuật
II	**Yêu cầu về phần cứng thiết bị tại Data Center**	
2.1	Thiết kế	Dạng Rack mout - tối thiểu 1U
2.2	Số lượng giao diện mạng	Tối thiểu 8 cổng GE RJ45 Tối thiểu 8 cổng 1GE SFP Tối thiểu 4 cổng 10GE SFP+
2.3	Nguồn điện	Có sẵn 2 nguồn , đảm bảo dự phòng về nguồn. Nguồn hỗ trợ khả năng thay thế nóng.
2.4	Hỗ trợ SSLVPN	≥ 2000 User
2.5	Thông lượng Firewall	≥ 130 Gbps
2.6	Thông lượng IPsec VPN	≥ 55 Gbps
2.7	Thông lượng IPS (Trong môi trường thực tế)	≥ 14 Gbps
2.8	Thông lượng NGFW (Trong môi trường thực tế)	≥ 22 Gbps
2.9	Thông lượng Threat Protection (Trong môi trường thực tế)	≥ 10.5 Gbps

STT	Yêu cầu kỹ thuật	Thông số kỹ thuật
2.10	Số lượng kết nối đồng thời (Concurrent Sessions)	≥ 8 Million
2.11	Số kết nối mới/giây (New Sessions/Second)	≥ 550.000
2.12	Số lượng Firewall ảo có sẵn	≥ 10
2.13	Chế độ dự phòng	Hỗ trợ Active-Active, Active-Passive, Clustering
2.14	Bảo hành và hỗ trợ kỹ thuật	3 năm bảo hành và hỗ trợ kỹ thuật
III	**Yêu cầu chung về tính năng WAN/SD-WAN cho các thiết bị Firewall**	
3.1	SD-WAN Controller On-premises	Thiết bị quản lý cấu hình, policy, monitoring, report, quản trị tập trung SD-WAN Router đặt tại TTDL
3.2	Hỗ trợ tính năng Zero Touch Provisioning	Triển khai cấu hình ban đầu tự động
3.3	Hỗ trợ giám sát mạng	Tính năng giám sát, đo kiểm chất lượng dịch vụ đường truyền theo thời gian thực
3.4	Hỗ trợ Per-flow/per-session/per-packet load balancing	Cân bằng tải đường truyền theo session
3.5	Hỗ trợ Smart QoS, bandwidth limitation	Áp dụng chính sách ưu tiên băng thông cho các ứng dụng quan trọng và tự động phát hiện mức băng thông sử dụng theo thời gian thực
3.6	Hỗ trợ tính năng Dynamic Path Switching/Dynamic traffic Steering	Tính năng tự động thay đổi đường đi kết nối tùy thuộc chất lượng đường truyền theo thời gian thực

STT	Yêu cầu kỹ thuật	Thông số kỹ thuật
3.7	Hỗ trợ tính năng Forward Error Connection (FEC)	Khắc phục mất gói tin qua đường truyền kém chất lượng
3.8	Hỗ trợ Data Encryption	Mã hóa dự liệu truyền dẫn trên đường truyền
3.9	Hỗ trợ tính năng Application visibility/ Application routing	Khả năng tự động nhận diện và định tuyến theo từng ứng dụng cụ thể
3.10	Hỗ trợ phân tích và giám sát	Phân tích luồng tin giúp kiểm soát băng thông đường truyền theo thời gian thực
3.11	Định tuyến OSPF	Hỗ trợ các giao thức định tuyến OSPF từ mạng WAN và mạng Core
3.12	Tính năng tường lửa	Tích hợp tính năng tường lửa (Firewall) kiểm soát truy cập tại đầu cuối
3.13	Hỗ trợ tính năng về WAN, SD-WAN	Cân bằng tải kết nối WAN/SD-WAN: WAN Optimization, Server Load Balancing
3.14	Bảo hành và hỗ trợ kỹ thuật	3 năm bảo hành và hỗ trợ kỹ thuật
IV	**Phần mềm quản lý tập trung**	
4.1	Giải pháp được cung cấp dưới dạng phiên bản phần mềm ảo hóa	Hỗ trợ cài đặt trên các hạ tầng ảo hóa như VMware ESX/ESXi, Microsoft Hyper-V Server, Citrix và Open Source XenServer, Linux KVM, Amazon AWS, GCP
4.2	Bản quyền phần mềm	Hỗ trợ quản lý lên tới 40 thiết bị tưởng lửa, có thể nâng cấp thêm khi cần
4.3	Tính năng quản lý thiết bị (Device Management)	Cho phép tự động khám phá hoặc thêm các thiết bị tường lửa bằng tay vào cơ sở dữ liệu
		Xem thông tin thiết bị tường lửa sau khi được thêm vào cơ sở dữ liệu, cho phép

STT	Yêu cầu kỹ thuật	Thông số kỹ thuật
		người quản trị chỉnh sửa thông tin trên thiết bị
		Cho phép hiển thị tối thiểu các thông tin trên thiết bị tường lửa bao gồm: hostname, IP address, firmware, license, configuration status
		Cho phép cấu hình và giám sát hoạt động tính năng sẵn sàng cao High Availability (HA)
		Cho phép truy nhập quản trị đến thiết bị tường lửa
4.4	Tính năng quản lý cấu hình (Configuration Management)	Hỗ trợ quản lý các phiên bản cấu hình trên thiết bị tường lửa, cho phép xem thông tin về từng phiên bản, so sánh sự khác biệt giữa các phiên bản
		Cho phép kiểm tra đồng bộ giữa cấu hình lưu trong cơ sở dữ liệu với cấu hình đang chạy trên thiết bị tường lửa
4.5	Tính năng quản lý chính sách (Policy Management)	Cho phép tạo các đối tượng (object) để định nghĩa chính sách (policy)
		Hỗ trợ tối thiểu các loại chính sách: IP, NAT, Proxy, Interface
4.6	Tính năng quản lý VPN	Cho phép cấu hình, giám sát và quản lý cả IPsec VPN và SSL VPN
		Hỗ trợ tạo IPSec VPN theo các mô hình: Full Meshed, Star hoặc Dial up
		Hỗ trợ giám sát trạng thái IPsec VPN
		Hỗ trợ các mẫu cấu hình có sẵn cho SSL VPN: Web-access, Tunnel-access, Full-access

STT	Yêu cầu kỹ thuật	Thông số kỹ thuật
4.7	Khả năng chia miền quản trị	Hỗ trợ tính năng chia nhiều miền quản trị để tăng khả năng vận hành hiệu quả
4.8	Tính năng vẽ lại Topology	Hỗ trợ tất cả các thiết bị tường lửa kết nối trong mạng của hệ thống, giúp giám sát nhanh chóng và dễ dàng
4.9	Hỗ trợ giao diện quản trị bản quyền phần mềm (license) cho các thiết bị tường lửa thế hệ mới có trong dự án này với các chức năng sau	Xuất báo cáo ở định dạng PDF về danh sách thiết bị, thông tin license, thông tin cập nhật chi tiết
		Hỗ trợ hiển thị danh sách thiết bị chi tiết theo các thông tin sau: tên thiết bị, số serial number, dòng sản phẩm, phiên bản Firmware
4.10	Hỗ trợ cơ chế hoạt động như máy chủ nội bộ cập nhật thông tin nhận diện cho các thiết bị tường lửa thế hệ mới có trong dự án này	Cập nhật database các tính năng Antivirus, IPS từ thiết bị quản lý tập trung tới các thiết bị tường lửa có trên toàn hệ thống
4.11	Bảo hành và hỗ trợ kỹ thuật	3 năm bảo hành và hỗ trợ kỹ thuật

Ghi chú:

- Bất kỳ hãng sản xuất, nhãn hiệu, ký mã hiệu (nếu có) trong bảng yêu cầu kỹ thuật chỉ nhằm mục đích mô tả và không nhằm mục đích hạn chế nhà thầu. Nhà thầu có thể lựa chọn dự thầu hàng hóa có nguồn gốc nhà sản xuất, nhãn hiệu, ký mã hiệu khác nhưng phải phù hợp với điều kiện cung cấp cũng như phải đảm bảo yêu cầu có tiêu chuẩn kỹ thuật, đặc tính kỹ thuật, tính năng sử dụng "tương đương" hoặc "cao hơn" so với các yêu cầu tối thiểu của E-HSMT. Nhà thầu phải cung cấp các tài liệu chứng minh sản phẩm chào thầu có tiêu chuẩn kỹ thuật, đặc tính kỹ thuật, tính năng sử dụng "tương đương" hoặc "cao hơn" so với các yêu cầu tối thiểu của E-HSMT.

Nhà thầu nộp Bảng tuyên bố đáp ứng chỉ tiêu kỹ thuật của hàng hóa chào thầu theo mẫu bên dưới:

MẪU BẢNG TUYÊN BỐ ĐÁP ỨNG CHỈ TIÊU KỸ THUẬT

STT	Yêu cầu của Chủ đầu tư		Nhà thầu chào			Ghi chú
	Nội dung	Yêu cầu kỹ thuật	Thông số kỹ thuật	Tuyên bố đáp ứng	Tài liệu tham chiếu	
1	Hàng hóa 1		Hàng hóa 1 (Ghi rõ ký mã hiệu SP/Hãng SX/Xuất xứ)			
	….	….	….	Ghi rõ Đáp ứng/Vượt trội hoặc Không đáp ứng	Nêu rõ tham chiếu tài liệu nào, chương, mục, trang, dòng nào hoặc đánh dấu highlight tại tài liệu kỹ thuật	
	….	….				
2	Hàng hóa 2		Hàng hóa 2 (Ghi rõ ký mã hiệu SP/Hãng SX/Xuất xứ)			
	….	….	…	Ghi rõ Đáp ứng/Vượt trội hoặc Không đáp ứng	Nêu rõ tham chiếu tài liệu nào, chương, mục, trang, dòng nào hoặc đánh dấu highlight tại tài liệu kỹ thuật	
	….	….	….			

1.2.3. Các yêu cầu phi chức năng:

1.2.3.1. Các yêu cầu về cài đặt, hạ tầng, đường truyền, an toàn vận hành, khai thác, sử dụng

Các thiết bị Firewall tại các KTNN Khu vực và tại Data Center được kết nối thiết lập hệ thống mạng WAN/SD-WAN. Các kết nối WAN được cấu hình VPN đảm bảo kết nối dữ liệu giữa các Khu vực và Data Center.

Thành phần giám sát, quản trị tập trung và lưu trữ log được cài đặt trên hệ thống máy chủ của KTNN, áp dụng các tiêu chuẩn kỹ thuật về an toàn, an ninh bảo mật của KTNN

Đường truyền sẽ được cấu hình SSL nhằm bảo đảm an toàn dữ liệu trong quá trình lưu chuyển trên mạng.

1.2.3.2. Yêu cầu về tính sẵn sàng với IPv6

Hệ thống được thiết kế và xây dựng sẽ đảm bảo tương thích và sẵn sàng với với IPv6 hoặc giải pháp nâng cấp bảo đảm sẵn sàng với IPv6 nếu hoạt động trên

môi trường Internet; trường hợp không kết nối Internet, khuyến khích khả năng tương thích hỗ trợ IPv6 hoặc có giải pháp nâng cấp bảo đảm sẵn sàng với IPv6

1.2.3.3. Yêu cầu về năng lực của cán bộ tham gia

Để đảm bảo tiến độ cũng như chất lượng hệ thống khi đưa vào triển khai theo kế hoạch. Yêu cầu tối thiểu năng lực của cán bộ tham gia như sau:

Có tối thiểu 02 nhân sự có chứng chỉ Architect về Network Security của hãng sản xuất thiết bị (PNCSE của Palo Alto hoặc NSE7/FCSS của Fortinet hoặc tương đương)

1.3. Yêu cầu khác:

1.3.1. Yêu cầu về triển khai

Sau khi kết thúc giai đoạn cài đặt và đào tạo chuyển giao công nghệ, đơn vị triển khai hệ thống phải có phương án hỗ trợ cho KTNN trong việc khai thác, sử dụng và quản trị vận hành hệ thống nhằm kịp thời xử lý ngay vấn đề xuất hiện trong quá trình hoạt động, đảm bảo hoạt động liên tục và an toàn, ổn định sau khi hệ thống đưa vào sử dụng.

Phạm vi và hình thức triển khai:

+ Phạm vi triển khai: Triển khai cài đặt hệ thống tại Trung tâm dữ liệu của KTNN và các KTNN khu vực.

+ Hình thức triển khai: Triển khai trực tiếp tại Trung tâm dữ liệu của KTNN và các KTNN khu vực.

1.3.2. Yêu cầu về bảo hành, bảo trì

- Thời hạn bảo hành, hỗ trợ kỹ thuật 3 năm theo tiêu chuẩn của hãng.

- Thời gian phản hồi (đối với sự cố nghiêm trọng) trong vòng 1h

- Thời gian phản hồi (đối với sự cố không nghiêm trọng) trong ngày làm việc tiếp theo

- Bảo hành thay thế thiết bị: trong thời gian bảo hành thiết bị, nếu thiết bị được hãng xác định là lỗi, hãng sẽ gửi thiết bị thay thế trước, khách hàng gửi lại thiết bị lỗi sau

- Hỗ trợ qua điện thoại

- Hỗ trợ qua website

- Được sử dụng công cụ hỗ trợ online

- Được cập nhật các bản vá của sản phẩm

Mục 2. Bản vẽ: Không có

Mục 3. Kiểm tra và thử nghiệm

- Kiểm tra, thử nghiệm sẽ được tiến hành khi hàng đến địa điểm bàn giao theo yêu cầu của E-HSMT.

- Chủ đầu tư sẽ trực tiếp kiểm tra, thử nghiệm hàng hóa với sự chứng kiến của nhà thầu.

- Trường hợp hàng hóa không phù hợp với đặc tính kỹ thuật theo hợp đồng thì Chủ đầu tư có quyền từ chối và nhà thầu phải có trách nhiệm thay thế hoặc tiến hành những điều chỉnh cần thiết để đáp ứng đúng các yêu cầu về đặc tính kỹ thuật. Trường hợp nhà thầu không có khả năng thay thế hay điều chỉnh hàng hóa không phù hợp. Chủ đầu tư có quyền tổ chức việc thay thế hay điều chỉnh nếu thấy cần thiết, mọi rủi ro và chi phí liên quan do Nhà thầu chịu. Việc thực hiện kiểm tra, thử nghiệm hàng hóa của Chủ đầu tư không dẫn đến miễn trừ nghĩa vụ bảo hành hay các nghĩa vụ khác theo hợp đồng của Nhà thầu.