TCCS

TIÊU CHUẨN CƠ SỞ

HIỆP HỘI AN TOÀN THÔNG TIN VIỆT NAM

VNISA
VIETNAM INFORMATION SECURITY ASSOCIATION

TCCS 01: 2019/VNISA
Xuất bản lần 01

TIÊU CHUẨN KỸ THUẬT VỀ GIẢI PHÁP HÓA ĐƠN ĐIỆN TỬ AN TOÀN

HÀ NỘI – 2019

Mục lục

Lời nói đầu

TCCS 01: 2019/VNISA – Tiêu chuẩn kỹ thuật về Giải pháp hóa đơn điện tử an toàn do Hiệp hội An toàn thông tin Việt Nam biên soạn và công bố. Câu lạc bộ Chữ ký số và Giao dịch điện tử Việt Nam (VCDC) là đơn vị giúp Hiệp hội xây dựng nội dung Tiêu chuẩn.

TCCS 01: 2019/VNISA được xây dựng trên cơ sở tham khảo tài liệu TCVN 11930 Công nghệ thông tin – Các kỹ thuật an toàn – Yêu cầu cơ bản về an toàn hệ thống thông tin theo cấp độ, và các văn bản quy phạm pháp luật liên quan tới phạm vi của tiêu chuẩn.

Lời giới thiệu

Hóa đơn là lĩnh vực hết sức quan trọng trong lĩnh vực tài chính, đó là cơ sở để tính toán tiền thuế mà mỗi doanh nghiệp, cá nhân cần hoàn thành nghĩa vụ nộp thuế với nhà nước. Hệ thống cung cấp Dịch vụ hóa đơn điện tử là hệ thống rất quan trọng bởi đây là hệ thống quản lý dữ liệu hóa đơn điện tử của các doanh nghiệp trong nhiều năm. Giải pháp Hóa đơn điện tử an toàn cần phải đảm bảo các tiêu chí về nghiệp vụ, tiêu chí về an toàn thông tin (ATTT) đảm bảo hạn chế đến mức cao nhất các rủi ro liên quan tới dữ liệu hóa đơn của doanh nghiệp.

Theo đề xuất của Câu lạc bộ Chữ ký số và Giao dịch điện tử Việt Nam, Hiệp hội An toàn Thông tin Việt Nam (VNISA) ban hành bộ tiêu chuẩn kỹ thuật (TCKT) giải pháp Hóa đơn điện tử (HĐĐT) an toàn với mục đích đưa ra các tiêu chí tối thiểu mà một giải pháp Hóa đơn điện tử nên có để đáp ứng:

- Các quy định của Nhà nước về ATTT.
- Các yêu cầu khách hàng về ATTT.
- Các tiêu chí về an toàn thông tin đang áp dụng cho các hệ thống phần mềm của VNISA.

Bộ TCKT làm sở cứ cho việc đánh giá, công nhận các giải pháp HĐĐT đạt tiêu chuẩn về ATTT theo tiêu chí của VNISA. Bộ TCKT bao gồm 05 phần:

- Phần 1: Phạm vi và đối tượng áp dụng
- Phần 2: Tài liệu liên quan
- Phần 3: Thuật ngữ viết tắt
- Phần 4: Nội dung Tiêu chuẩn kỹ thuật
- Phần 5: Phụ lục

Hệ thống cung cấp dịch vụ HĐĐT được VNISA định nghĩa tương đương với hệ thống thông tin cấp độ 3 (level 3) là hệ thống mà khi bị phá hoại sẽ làm tổn hại nghiêm trọng tới sản xuất, lợi ích công cộng và trật tự, an toàn xã hội hoặc làm tổn hại tới quốc phòng, anh ninh quốc gia (TCVN 11930).

Các TCKT sử dụng để đánh giá giải pháp HĐĐT an toàn kế thừa có bổ sung các TCKT liên quan, phù hợp về mặt tổng thể với các quy định của nhà nước trong cùng lĩnh vực.

Hệ thống được đánh giá là Đạt khi: Đáp ứng 100% các yêu cầu của bộ TCKT.

Tiêu chuẩn kỹ thuật về giải pháp hóa đơn điện tử an toàn

1 Phạm vi và đối tượng áp dụng

- Phạm vi:
  + Tài liệu này được áp dụng trong các hoạt động kiểm tra, đánh giá, chứng nhận và truyền thông, đào tạo...của VNISA. VNISA sử dụng tài liệu như tiêu chuẩn cơ sở của Hiệp hội trong các hoạt động chuyên môn theo quy định của pháp luật.
  + Tài liệu có tính chất tham khảo để các tổ chức, cá nhân vận dụng vào các hoạt động xây dựng, lựa chọn, hoàn thiện giải pháp HĐĐT.
- Đối tượng áp dụng:
  + Các tổ chức, cá nhân là thành viên của VNISA có liên quan trong lĩnh vực cần tuân thủ chấp hành các nội dung được đề cập trong TCCS.
  + Các Doanh nghiệp, cá nhân, tổ chức sử dụng như tài liệu tham khảo trong việc xây dựng, lựa chọn, đánh giá tính ATTT của giải pháp HĐĐT an toàn.

2 Tài liệu tham chiếu

- Nghị định 26/2007/NĐ-CP Quy định thi hành luật giao dịch điện tử về Chữ ký số và Dịch vụ Chứng thực Chữ ký số.
- Thông tư 06/2015/TT-BTTTT Quy định danh mục tiêu chuẩn bắt buộc áp dụng về chữ ký số và dịch vụ chứng thực chữ ký số.
- Thông tư 32/2011/TT-BTC Hướng dẫn về khởi tạo, phát hành và sử dụng Hóa đơn điện tử bán hàng hóa và cung ứng dịch vụ.
- Nghị Định 119/2018/NĐ-CP Quy định về hóa đơn điện tử khi bán hàng hóa, cung cấp dịch vụ
- TCVN 11930: 2017 Công nghệ thông tin – Các kỹ thuật an toàn – Yêu cầu cơ bản về an toàn hệ thống thông tin theo cấp độ.

3 Thuật ngữ viết tắt

ATTT	An toàn thông tin
CSDL	Cơ sở dữ liệu (Database)
CCID (protocol)	Chuẩn giao thức USB cho phép thiết bị thẻ thông minh kết nối với máy tính qua giao diện USB (Chip card interface device)
FIPS	Là các tiêu chuẩn do Chính phủ liên bang Hoa Kỳ phát triển và công bố sử dụng trong các hệ thống máy tính bởi cơ quan phi chính phủ và các nhà thầu chính phủ (Federal Information Processing Standard)
HĐĐT	Hóa đơn điện tử
HSM	Thiết bị phần cứng bảo mật chuyên dụng dùng để tạo, lưu trữ và bảo vệ khóa quan trọng của CA và SubCA (Hardware Security Module)
HA	Là đặc điểm của một hệ thống nhằm đảm bảo mức độ hiệu quả hoạt

	động đảm bảo trong khoảng thời gian hoạt động bình thường và thời gian cao tải (High Availability)
IP	Mã bảo vệ quốc tế (International Protection)
NĐ	Nghị định
NĐ-CP	Nghị định chính phủ
PC	Máy vi tính cá nhân (Personal Computer)
PCCC	Phòng cháy chữa cháy
SHA	Hàm băm an toàn (Secure Hash Algorithm)
TCKT	Tiêu chuẩn kỹ thuật
TCVN	Tiêu chuẩn Việt Nam
TT-BTTTT	Thông tư Bộ thông tin và truyền thông
TT	Thông tư
TT-BTC	Thông tư Bộ tài chính

4 Nội dung Tiêu chuẩn kỹ thuật

4.1 Mô tả chung

Hóa đơn là chứng từ kế toán do tổ chức, cá nhân bán hàng hóa, cung cấp dịch vụ lập, ghi nhận thông tin bán hàng hóa, cung cấp dịch vụ theo quy định của luật kế toán.

Hóa đơn điện tử là hóa đơn được thể hiện ở dạng dữ liệu điện tử do tổ chức, cá nhân bán hàng hóa, cung cấp dịch vụ lập, ghi nhận thông tin bán hàng hóa, cung cấp dịch vụ, ký số, ký điện tử theo quy định bằng phương tiện điện tử, bao gồm cả trường hợp hóa đơn được khởi tạo từ máy tính tiền có kết nối chuyển dữ liệu điện tử với cơ quan thuế.

Giải pháp Hóa đơn điện tử là giải pháp về hệ thống phần mềm, phần cứng, quy trình để triển khai cho phép doanh nghiệp khởi tạo, lập, gửi, nhận, lưu trữ và quản lý Hóa đơn bằng phương tiện điện tử.

Yêu cầu về Hệ thống cho Giải pháp hóa đơn điện tử cần đáp ứng các tiêu chí:

- Tính đầy đủ các chức năng nghiệp vụ HĐĐT theo quy định của nhà nước
- ATTT máy chủ
- ATTT phần mềm, ứng dụng, bảo vệ dữ liệu.
- ATTT vật lý
- Tổ chức và Nhân sự
- Các tiêu chí khác (được chi tiết hóa...)

4.2 Các phương pháp đánh giá và đo lường chuẩn

a. Phương pháp đánh giá: kiểm tra hoạt động thực tiễn của các chức năng, của hệ thống, giải pháp

- Nguyên tắc đánh giá: Dựa trên việc kiểm tra, đo lường kết quả hoạt động của các chức năng của hệ thống, giải pháp có đạt mức phù hợp với yêu cầu, chỉ tiêu, tiêu chuẩn được công bố.
- Mục đích áp dụng để đánh giá: Tính phù hợp, tính chính xác của chức năng theo các tiêu chí được đề ra.
- Phương thức thực hiện: Chạy thử trên thực tế, mọi tình huống, kiểm tra chức năng, tổng hợp kết quả đánh giá.

b. Phương pháp đánh giá: Lấy ý kiến của chuyên gia

- Nguyên tắc đánh giá: Dựa trên ý kiến nhận xét của các chuyên gia hàng đầu hoặc Hội đồng chuyên gia chuyên ngành trên cơ sở kinh nghiệm và phân tích tài liệu hồ sơ và biên bản vận hành của hệ thống
- Mục đích áp dụng: Có thể áp dụng để đánh giá các tiêu chí phi chức năng như: Tính bảo mật, kiến trúc công nghệ, khả năng bảo trì, khả năng tương tác, khả năng phân tích, khả năng thay đổi được, khả năng cài đặt phần mềm, khả năng chịu lỗi, khả năng phục hồi, khả năng tương thích, chất lượng mã nguồn.
- Phương thức thực hiện: Tổng hợp ý kiến chuyên gia nhận xét đánh giá các tài liệu giải pháp, công nghệ áp dụng, hồ sơ hệ thống và kết quả vận hành thử nghiệm trên thực tiễn.

c. Các phương pháp khác

- Tùy theo tình hình thực tế, xem xét áp dụng bổ sung không giới hạn các phương pháp khác phù hợp với đối tượng và mục tiêu đánh giá.
- Các phương pháp bổ sung này phải được mô tả đầy đủ trong báo cáo tại các mục tiêu chí đánh giá liên quan.

4.3 Mô tả chi tiết các yêu cầu bắt buộc

TT	Nội dung đánh giá	Phương pháp đánh giá			Tài liệu tham chiếu (nếu có)
		Các tiêu chí cơ bản	Quy trình thực hiện	Kết quả cần đạt được	
I	**Đầy đủ chức năng nghiệp vụ HĐĐT**				
1.1	Chức năng khởi tạo HĐĐT	Là các chức năng đáp ứng các nghiệp vụ để dịch vụ HĐĐT hoạt động theo đúng quy định của Nhà nước về hóa đơn điện tử. Chức năng ký số và xác thực cần đáp ứng các yêu cầu: Ký và xác thực với tất cả các nhà cung cấp hợp pháp được công nhận theo quy định pháp luật. Ký và xác thực theo quy định pháp luật. Chức năng ký số áp dụng thuật toán hàm băm tối thiểu SHA1 trở lên.	Áp dụng phương pháp đánh giá, kiểm tra hoạt động thực tiễn của các chức năng.	Các chức năng có đầy đủ và thực hiện đúng nghiệp vụ.	NĐ19, TT32, NĐ 130
1.2	Chức năng lập HĐĐT				
1.3	Chức năng gửi, nhận HĐĐT				
1.4	Chức năng lưu trữ HĐĐT				
1.5	Chức năng quản lý HĐĐT: tìm kiếm, thay thế, điều chỉnh Hóa đơn điện tử				
1.6	Chức năng ký số trên HĐĐT				
1.7	Chức năng xác thực chữ ký số trên HĐĐT	Chức năng ký số và xác thực cần đáp ứng các yêu cầu: Ký và xác thực với tất cả các nhà cung cấp hợp pháp được công nhận theo quy định pháp luật. Ký và xác thực theo quy quy định pháp luật.	Áp dụng phương pháp đánh giá, kiểm tra hoạt động thực tiễn của các chức năng	Các chức năng có đầy đủ và thực hiện đúng nghiệp vụ.	
II	**Bảo đảm an toàn máy chủ, thiết bị hệ thống**				

2.1	**Xác thực và Kiểm soát truy cập**				
	Thiết lập chính sách xác thực người dùng khi truy cập, quản lý và sử dụng máy chủ và thiết bị hệ thống (nếu thiết bị có chức năng xác thực).	Là các chính sách xác thực người dùng quản trị khi truy cập máy chủ hệ thống.	Áp dụng phương pháp đánh giá, kiểm tra hoạt động thực tiễn của các chức năng	Hệ thống có các thiết lập chính sách quản trị người dùng	**TCVN 11930**
	Thay đổi hoặc vô hiệu hóa các tài khoản mặc định, cổng quản trị mặc định (nếu có).	Không cho phép các tài khoản mặc định, cổng quản trị mặc định hoạt động khi không được phép.	Áp dụng phương pháp đánh giá, kiểm tra hoạt động thực tiễn của các chức năng	Hệ thống vô hiệu hóa các tài khoản, cổng quản trị mặc định.	**TCVN 11930**
	Yêu cầu sử dụng mật khẩu mạnh hoặc có sử dụng các phần mềm công cụ giúp quản trị viên quản lý mật khẩu của hệ thống.	Thay đổi mật khẩu mặc định Thiết lập mật khẩu mạnh Thời gian thay đổi mật khẩu định kỳ < 3 tháng Số lần nhập sai mật khẩu	Áp dụng phương pháp đánh giá, kiểm tra hoạt động thực tiễn của các chức năng	Hệ thống áp dụng chính sách mật khẩu mạnh.	**TCVN 11930**
	Thiết lập các chính sách về quản lý truy cập, IP được truy cập, thời gian truy cập,… đến các máy chủ và thiết bị của hệ thống khi vận hành từ xa.	Giới hạn, kiểm soát các thông tin truy cập tới máy chủ: IP, thời gian, số lượng truy cập.	Áp dụng phương pháp đánh giá, kiểm tra hoạt động thực tiễn của các chức năng	Hệ thống có chính sách quản lý truy cập, cấu hình kiểm soát truy cập.	**TCVN 11930**
2.2	**Nhật ký hệ thống**				
	Nhật ký hệ thống cần lưu trữ đầy đủ các thông tin cơ bản sau: Log tường lửa, thông tin đăng nhập vào máy chủ, thiết bị, thông tin tác động của người	Lưu đầy đủ thông tin các hoạt động tác động đến máy chủ trong thời gian quy định, phục vụ việc truy vết, xác định nguyên nhân vụ việc.	Áp dụng phương pháp đánh giá, kiểm tra hoạt động thực tiễn của các chức năng. Kết hợp phương pháp đánh giá,	Hệ thống có đầy đủ các Log tác động.	**TCVN 11930**

	dùng trong phiên đăng nhập. Các thông tin trên lưu tối thiểu trong thời gian 3 tháng gần nhất (so với thời điểm đánh giá).		lấy ý kiến của chuyên gia		
2.3	**Phòng chống xâm nhập, phần mềm độc hại**				
	Sử dụng tường lửa (firewall) để ngăn chặn các truy cấp trái phép tới máy chủ, thiết bị của hệ thống.	Quản lý, kiểm soát kết nối hợp pháp.	Áp dụng phương pháp đánh giá, kiểm tra hoạt động thực tiễn của các chức năng	Có sử dụng tường lửa, có cấu hình ngăn chặn truy cập bất hợp pháp.	**TCVN 11930**
	Sử dụng các giao thức mạng an toàn. Vô hiệu hóa các giao thức mạng không an toàn, các dịch vụ mặc định không sử dụng của máy chủ, thiết bị.	Máy tính (windows server, Linux …) thường có các giao thức mạng, các dịch vụ mặc định. Nếu không sử dụng thì phải vô hiệu hóa các thông tin này để tránh bị lợi dụng lỗ hổng.	Áp dụng phương pháp đánh giá, kiểm tra hoạt động thực tiễn của các chức năng	Vô hiệu hóa các giao thức mạng, dịch vụ mặc định không sử dụng cho dịch vụ.	**TCVN 11930**
	Có phương án cập nhật bản nâng cấp, bản vá lỗi của hệ điều hành và các dịch vụ đi kèm máy chủ, thiết bị.	Có phương án, kế hoạch cập nhật thường xuyên bản vá hệ điều hành.	Áp dụng phương pháp đánh giá, kiểm tra hoạt động thực tiễn của các chức năng. Kết hợp phương pháp đánh giá, lấy ý kiến của chuyên gia	Có phương án khả thi.	**TCVN 11930**

	Máy chủ cài đặt phần mềm diệt Virus, phần mềm phòng chống mã độc hại.	Có sử dụng phần mềm diệt virus bản quyền.	Áp dụng phương pháp đánh giá, kiểm tra hoạt động thực tiễn của các chức năng.	Có cài đặt.	**TCVN 11930**
	Có chính sách định kỳ dò quét và xử lý phần mềm độc hại, điểm yếu ATTT.	Có quy trình, quy định định kỳ dò quét và xử lý phần mềm độc hại, điểm yếu ATTT.	Áp dụng phương pháp đánh giá, lấy ý kiến của chuyên gia	Có quy trình, quy định dò quét và xử lý.	**TCVN 11930**
	Máy chủ cài đặt phần mềm có bản quyền (hệ điều hành, cơ sở dữ liệu).	Phần mềm có bản quyền đảm bảo thường xuyên cập nhật các tính năng mới, bản vá lỗi, và đảm bảo ATTT hơn.	Áp dụng phương pháp đánh giá, kiểm tra hoạt động thực tiễn của các chức năng.	Có bản quyền của Hệ điều hành và các phần mềm sử dụng trên hệ thống.	**TCVN 11930**
2.4	**Xử lý máy chủ, thiết bị khi chuyển giao mục đích sử dụng**				
	Có phương án xóa, dự phòng dữ liệu khi không còn sử dụng. Đảm bảo dữ liệu không thể phục hồi sau khi xóa.	Các máy chủ không còn sử dụng, chuyển giao mục đích sử dụng hoặc tiêu hủy cần đảm bảo các dữ liệu trong đó không thể bị khôi phục.	Áp dụng phương pháp đánh giá, lấy ý kiến của chuyên gia.	Có quy trình, quy định xử lý.	**TCVN 11930**
III	**Bảo đảm an toàn phần mềm, ứng dụng, lưu trữ và bảo mật dữ liệu**				
3.1	**Xác thực, kiểm soát truy cập**				
	Lưu trữ mã hóa các thông tin nhạy cảm.	Các thông tin nhạy cảm phải được mã hóa trong CSDL: mật khẩu, mã bí mật,…	Áp dụng phương pháp đánh giá, kiểm tra hoạt động thực tiễn của các chức năng.	Các thông tin nhạy cảm phải được mã hóa trong CSDL.	**TCVN 11930**
	Đảm bảo an toàn mật khẩu người sử dụng gồm:	Thay đổi mật khẩu mặc định Thiết lập mật khẩu mạnh	Áp dụng phương pháp đánh giá, kiểm tra hoạt	Có áp dụng chính sách mật khẩu mạnh.	**TCVN 11930**

	Thay đổi mật khẩu mặc định Sử dụng mật khẩu mạnh Thiết lập thời gian thay đổi mật khẩu Số lần nhập sai mật khẩu.	Thời gian thay đổi mật khẩu định kỳ < 3 tháng Số lần nhập sai mật khẩu.	động thực tiễn của các chức năng.		
	Thiết lập thời gian ngắt kết nối khi không có yêu cầu từ người dùng.	Giới hạn thời gian truy cập.	Áp dụng phương pháp đánh giá, kiểm tra hoạt động thực tiễn của các chức năng.	Ứng dụng có thiết lập thông số thời gian ngắt kết nối.	**TCVN 11930**
	Thiết lập phân quyền người dùng mức dữ liệu.	Đảm bảo ATTT mức dữ liệu, tránh tấn công Cross-Site Request Forgery (CSRF).	Áp dụng phương pháp đánh giá, kiểm tra hoạt động thực tiễn của các chức năng.	Ứng dụng có phân quyền mức dữ liệu.	**TCVN 11930**
3.2	**Nhật ký hệ thống**				
	Ghi, lưu trữ nhật ký hệ thống trong thời gian tối thiểu 03 tháng, với các thông tin cơ bản sau: Thông tin truy cập ứng dụng Lỗi phát sinh hệ thống - Thông tin tác động, cấu hình từ quản trị viên.	Lưu đầy đủ thông tin các hoạt động tác động đến ứng dụng trong thời gian quy định, phục vụ việc truy vết, xác định nguyên nhân vụ việc.	Áp dụng phương pháp đánh giá, kiểm tra hoạt động thực tiễn của các chức năng.	Ứng dụng có đầy đủ các Log tác động.	**TCVN 11930**
	Nhật ký về các tác động lập, sửa, xóa, hủy hóa đơn điện tử phải được lưu trữ trong thời gian tối thiểu 10 năm kể từ thời điểm thực hiện thành	Đảm bảo tính pháp lý của dịch vụ khi xảy ra tranh chấp.	Áp dụng phương pháp đánh giá, kiểm tra hoạt động thực tiễn của các chức năng.	Có ghi nhật ký và đơn vị được đánh giá chứng minh khả năng lưu trữ tối thiểu 10 năm.	**TCVN 11930**

	công giao dịch.				
3.3	**An toàn ứng dụng và mã nguồn, bảo mật dữ liệu**				
	Mã hóa các thông tin nhạy cảm, bí mật khi lưu trữ, khi truyền thông tin qua các kênh kết nối.	Các thông tin nhạy cảm phải được mã hóa khi lưu trữ, khi truyền tải.	Áp dụng phương pháp đánh giá, kiểm tra hoạt động thực tiễn của các chức năng.	Ứng dụng có mã hóa thông tin nhạy cảm.	**TCVN 11930**
	Có phương án bảo vệ ứng dụng chống lại các tấn công phổ biến như: SQL Injection, OS Command injection, XSS, CSRF, RFI, LFI, Xpath injection.	Chống các tấn công phổ biến hiện nay đến ứng dụng.	Áp dụng phương pháp đánh giá, kiểm tra hoạt động thực tiễn của các chức năng.	Ứng dụng khắc phục các lỗ hổng trên.	**TCVN 11930**
	Có chức năng thông báo lỗi cho người dùng.	Khi có lỗi xảy ra phải thông báo rõ ràng đầy đủ nguyên nhân lỗi và cách xử lý với lỗi cho người dùng.	Áp dụng phương pháp đánh giá, kiểm tra hoạt động thực tiễn của các chức năng.	Có thông báo thông tin lỗi.	**TCVN 11930**
	Sử dụng chữ ký số để chống chối bỏ, xác thực các dữ liệu, thông tin quan trọng theo quy định.	Hàm băm SHA1 trở lên, thuật toán ký RSA.	Áp dụng phương pháp đánh giá, kiểm tra hoạt động thực tiễn của các chức năng. Kết hợp phương pháp đánh giá, lấy ý kiến của chuyên gia	Áp dụng đúng các thuật toán, thư viện SHA, RSA.	**TT 06/2015/TT-BTTTT**
3.4	**Sao lưu dự phòng, bảo đảm an toàn dữ liệu**				

	Có chính sách sao lưu dự phòng dữ liệu, log tác động, hệ diều hành định kỳ.	Có quy trình sao lưu dữ liệu 10 năm, sao lưu hàng ngày, dữ liệu lưu trữ 3 tháng gần nhất.	Áp dụng phương pháp đánh giá, lấy ý kiến của chuyên gia.	Có chính sách sao lưu dữ liệu.	
	Đường internet: Đường chính và dự phòng tối thiểu 10MB.	Đảm bảo tính sẵn sàng của hệ thống. (10MB đáp ứng 8 triệu hóa đơn phát hành 1 ngày).	Áp dụng phương pháp đánh giá, lấy ý kiến của chuyên gia.	Có tối thiểu 2 đường truyền có tốc độ theo quy định.	
	Thiết bị lữu trữ Chứng thư số: thiết bị USB Token, HSM hoặc các thiết bị tương đương đảm bảo tiêu chuẩn của nhà nước.	USB Token đạt tối thiểu FIPS2 trở lên. HSM đạt tối thiểu FIPS3 trở lên.	Áp dụng phương pháp đánh giá, lấy ý kiến của chuyên gia.	Có lưu trữ chứng thư số trên HSM hoặc thiết bị tương đương.	**TT 06/2015/TT-BTTTT**
	Hệ thống tường lửa, IPS/IDS có khả năng phát hiện, cảnh báo và ngăn chặn các truy cập bất hợp pháp, các hình thức tấn công trên môi trường mạng.	Đảm bảo tính bảo mật cho hệ thống.	Áp dụng phương pháp đánh giá, lấy ý kiến của chuyên gia.	Có hệ thống tường lửa và IPS/IDS tương đương phát hiện được tấn công dò quét khi thử nghiệm.	
	Hệ thống máy chủ cài đặt theo công nghệ cluster, load balancing, quản trị từ xa. Có cán bộ trực hệ thống 24/7. Có điện thoại hỗ trợ KH.	Tiêu chí này đảm bảo tính sẵn sàng cao (HA) của hệ thống, khi có 1 phần hệ thống, hạ tầng gặp sự cố.	Áp dụng phương pháp đánh giá, lấy ý kiến của chuyên gia.	Máy chủ có dự phòng, có hệ thống lưu trữ dữ liệu đủ thời gian tối thiểu 10 năm, có nhân sự trực 24/7.	**ISO27001**
	Hệ thống UPS, hệ thống máy phát điện đảm bảo hoạt động hệ thống 24/7.	Tiêu chí này đảm bảo tính sẵn sàng cao (HA) của hệ thống khi có sự cố về điện.	Áp dụng phương pháp đánh giá, kiểm tra hoạt động thực tiễn của các chức năng.	Hệ thống UPS hoạt động trực tuyến: Khi ngắt điện hệ thống UPS hoạt động và kích hoạt máy phát điện	

				hoạt động.	
IV	**An toàn thông tin vật lý**				
	Có hệ thống camera an ninh giám sát phòng máy.	Đảm bảo an ninh vật lý.	Áp dụng phương pháp đánh giá, kiểm tra hoạt động thực tiễn của các chức năng.	Có hệ thống Camera hoạt động tốt, có khả năng xem lại dữ liệu trong vòng tối thiểu 1 tháng từ ngày kiểm tra.	
	Có các phương án và hệ thống dự phòng đảm bảo duy trì hoạt động an toàn, liên tục và có các phương án xử lý tình huống bất thường, khắc phục sự cố: quy trình phục hồi dữ liệu khi gặp sự cố; thời gian phục hồi dữ liệu tối đa 08 giờ kể từ thời điểm hệ thống gặp sự cố.	Đảm bảo tính sẵn sàng khi có sự cố.	Áp dụng phương pháp đánh giá, lấy ý kiến của chuyên gia.	Có quy trình văn bản hóa thử nghiệm một quy trình thực tế để đảm bảo quy trình phù hợp và có hiệu lực.	**TCVN 11930**
	Các yêu cầu đảm bảo an toàn PCCC: Có hệ thống báo cháy, báo nổ, chống sét, có hệ thống điều hòa tập trung.	Đảm bảo an toàn cho hệ thống.	Áp dụng phương pháp đánh giá, lấy ý kiến của chuyên gia.	Có hệ thống báo cháy, báo khói Có hệ thống điều hòa tập trung.	**TCVN 11930**
	Có hệ thống dự phòng thảm họa (DR) đặt cách xa hệ thống chính 20Km.	Hệ thống dự phòng thảm họa (DR) đảm bảo khoảng cách tối thiểu 20 Km so với hệ thống chính.	Áp dụng phương pháp đánh giá, lấy ý kiến của chuyên gia.	Có hệ thống dự phòng thảm họa (DR) với các tính năng đầy đủ như hệ thống chính.	**TCVN 11930**

V	**Yêu cầu Tổ chức**				
	Có tối thiểu 05 năm hoạt động trong lĩnh vực công nghệ thông tin.				**TT 06**
	Đã triển khai hệ thống, ứng dụng công nghệ thông tin cho tối thiểu 10 tổ chức				**TT 06**
	Có cam kết bảo lãnh của tổ chức tín dụng hoạt động hợp pháp tại Việt Nam với giá trị trên 5 tỷ đồng để giải quyết các rủi ro và bồi thường thiệt hại có thể xảy ra trong quá trình cung cấp dịch vụ				
VI	**Yêu cầu Nhân sự**				
	Có tối thiểu 20 cán bộ kỹ thuật trình độ đại học chuyên ngành về công nghệ thông tin.		Áp dụng phương pháp đánh giá, lấy ý kiến của chuyên gia.	Cung cấp bằng cấp, chứng nhận hợp lệ.	
	Các cán bộ phụ trách ATTT của tổ chức phải có trình độ, chuyên ngành về CNTT, an toàn thông tin, phù hợp với vị trí tuyển dụng.	Tối thiểu phải có 1 cán bộ phụ trách được đào tạo về ATTT (Có bằng đại học chuyên ngành ATTT hoặc chứng chỉ về ATTT như CEH, Sec+ hoặc ECSA, LPT,… hoặc tương đương) và có kinh nghiệm tối thiểu 2 năm trong lĩnh vực ATTT.	Áp dụng phương pháp đánh giá, lấy ý kiến của chuyên gia.	Cung cấp bằng cấp, chứng nhận, tài liệu hợp lệ.	

	Cán bộ phụ trách quản trị mạng phải có trình độ đại học, chuyên ngành CNTT	Tối thiểu phải có 1 cán bộ phụ trách quản trị mạng có chứng chỉ quản trị mạng (CCNA, MCSA hoặc CEH…hoặc tương đương).	Áp dụng phương pháp đánh giá, lấy ý kiến của chuyên gia.	Cung cấp bằng cấp, chứng nhận, tài liệu hợp lệ.	
	Có quy định, quy trình đảm bảo ATTT liên quan tới hệ thống cung cấp dịch vụ HĐĐT của đơn vị.	Có văn bản ban hành quy định	Áp dụng phương pháp đánh giá, lấy ý kiến của chuyên gia.	Quy định, quy trình.	
	Cán bộ kỹ thuật có cam kết giữ bí mật thông tin liên quan tới tổ chức sau khi nghỉ việc.	Có văn bản ban hành quy định và cam kết	Áp dụng phương pháp đánh giá, lấy ý kiến của chuyên gia.	Các bản cam kết đã ký	
VII	**Các tiêu chí khác**				
	Thời gian dừng hệ thống để bảo trì không quá 2% tổng số giờ cung cấp dịch vụ.	Có văn bản quy định.	Áp dụng phương pháp đánh giá, lấy ý kiến của chuyên gia.	Mô tả đầy đủ phương án kỹ thuật khả thi đểđáp ứng yêu cầu.	

5 Phụ lục

5.1 Mẫu đánh giá Chức năng, nghiệp vụ của Giải pháp

MẪU ĐÁNH GIÁ CHỨC NĂNG NGHIỆP VỤ CỦA GIẢI PHÁP (Các yêu cầu bắt buộc)						
TCKT	**Bài đo và kết quả**					
	Các chỉ tiêu	**Kết quả mong muốn**	**Thực tế**	**Có**	**Không**	**Kết luận**
1. Đầy đủ các chức năng						
Chức năng khởi tạo HĐĐT	Tạo mẫu hóa đơn	Hệ thống có các chức năng để Hỗ trợ doanh nghiệp sử dụng được Hóa đơn điện tử.				
	Tạo quyết định sử dụng hóa đơn điện tử					
	Tạo thông báo phát hành hóa đơn					
Chức năng lập HĐĐT	Tạo hóa đơn trực tiếp từ phần mềm HDDT	Có đầy đủ các chức năng				
	Tạo hóa đơn từ dữ liệu Excel					
	Tạo hóa đơn qua API tích hợp với phần mềm kế toán bán hàng					
Chức năng gửi, nhận HĐĐT	Gửi hóa đơn qua email/ tin nhắn	Có chức năng				

Chức năng lưu trữ HĐĐT	Lưu hóa đơn trên máy tính của khách hàng.	Có chức năng				
Chức năng quản lý HĐĐT: tìm kiếm, thay thế, điều chỉnh HDDT.		Có chức năng				
Chức năng ký số trên HĐĐT	Chức năng ký số cho người bán	Có chức năng và ký được với tất cả các chữ ký số của các nhà cung cấp khác nhau				
	Chức năng ký số cho người mua					
Chức năng xác thực chữ ký số trên HĐĐT	Chức năng trình bày được thư mục hóa đơn có định dạng XML	Có chức năng và xác thực được Chữ ký số trên định dạng XML				

5.2 Mẫu đánh giá an toàn thông tin hệ thống máy chủ

MẪU ĐÁNH GIÁ AN TOÀN THÔNG TIN MÁY CHỦ (Các yêu cầu bắt buộc)						
TCKT	**Bài đo và kết quả**					
	Các chỉ tiêu	**Kết quả mong muốn**	**Thực tế**	**Có**	**Không**	**Kết luận**
1. Xác thực và Kiểm soát truy cập						
Thiết lập chính sách xác thực người dùng khi truy cập, quản lý và sử dụng máy chủ và thiết bị hệ thống (nếu thiết bị có chức năng xác thực).	Xác thực bằng tài khoản/mật khẩu	Hệ thống có các thiết lập các chính sách người dùng quản trị.				
	Xác thực bằng OTP					
	Xác thực bằng Chữ ký số					
	Khác					
Thay đổi hoặc vô hiệu hóa các tài khoản mặc định, cổng quản trị mặc định của máy chủ dịch vụ và DB (nếu có)	Đã đóng hoặc thay đổi cổng dịch vụ SSH 22	Hệ thống vô hiệu hóa các tài khoản, cổng quản trị mặc định.				
	Đã đóng hoặc thay đổi cổng dịch vụ Microsoft RDP 3389					

	Đã đóng hoặc thay đổi cổng dịch vụ Telnet 23	22				
	Đã đóng hoặc thay đổi cổng dịch vụ IHS Administration 8008					
	Đã đóng hoặc thay đổi cổng dịch vụ Jonas Admin Console 9000					
	Đã đóng hoặc thay đổi cổng dịch vụ WildFly Admin Console 9990					
	Đã đóng hoặc thay đổi cổng dịch vụ WebLogic Admin Console	7001				
	Đã đóng hoặc thay đổi cổng dịch vụ WAS Admin Console (SSL)	9043				
	Đã đóng hoặc thay đổi cổng dịch vụ WAS Admin Console	9060				
	Đã đóng hoặc thay đổi cổng dịch vụ JBoss Admin Console 8080					
Yêu cầu sử dụng mật khẩu mạnh hoặc có sử dụng các phần mềm công	Đã thiết lập chính sách mật khẩu phải bao gồm chữ hoa, chữ thường, ký tự đặc biệt và dài hơn 8 ký tự (Hoặc sử dụng	Hệ thống áp dụng chính sách mật khẩu mạnh.				

cụ giúp quản trị viên quản lý mật khẩu của hệ thống.	phần mềm quản lý và tạo mật khẩu).					
	Đã thiết lập chính sách bắt buộc 3 tháng thay đổi mật khẩu một lần.					
Thiết lập các chính sách về quản lý truy cập, IP được truy cập, thời gian truy cập,... đến các máy chủ và thiết bị của hệ thống khi vận hành từ xa.	Đã thiết lập xác thực IP truy cập cho các thiết bị máy chủ truy cập từ xa.	Hệ thống có chính sách, cấu hình kiểm soát.				
	Đã giới hạn 5 lần truy cập thất bại sẽ bị khóa và gửi cảnh báo đến quản trị viên: SMS hoặc email.					
	Đã giới hạn thời ngắt kết nối khi không có thao tác (quá 5 phút).					
2.Nhật ký hệ thống						
Nhật ký hệ thống cần lưu trữ đầy đủ các thông tin cơ bản sau: Log tường lửa, thông tin đăng nhập vào máy chủ, thiết bị, thông tin tác động của người dùng trong phiên đăng nhập. Các thông tin trên lưu tối thiểu trong	Đã lưu log IPS/IDS	Có lưu log				
	Đã lưu log tường lửa					
	Đã lưu log đăng nhập hệ thống					
	Đã lưu log thay đổi cấu hình của quản trị	Hệ thống có thể lưu đầy đủ nhật ký, sự kiện an toàn thông tin.				
	Thời gian lưu trữ log tối thiểu 3 tháng tính từ ngày kiểm tra.					

thời gian 3 tháng gần nhất (so với thời điểm đánh giá).						
3. Phòng chống xâm nhập, phần mềm độc hại						
Sử dụng tường lửa (fiewall) để ngăn chặn các truy cập trái phép tới máy chủ, thiết bị của hệ thống.	Đã thiết lập các luật chặn cho máy chủ, thiết bị của hệ thống trên tường lửa theo mô hình hệ thống.	Có sử dụng tường lửa, có cấu hình ngăn chặn truy cập bất hợp pháp.				
Sử dụng các giao thức mạng an toàn. Vô hiệu hóa các giao thức mạng không an toàn, các dịch vụ mặc định không sử dụng của máy chủ, thiết bị.	Đã vô hiệu hóa HTTP					
	Đã vô hiệu hóa Ping, Telnet					
	Đã vô hiệu hóa: TLS 1.1					
	Đã vô hiệu hóa, TLS 1.0, TLS 1.1					
	Đã sử dụng giao thức an toàn: HTTPS (Khuyến nghị nên chuyển sang giao thức TLS v2)					
	Đã sử dụng các giao thức an toàn: TLS v2	Vô hiệu hóa các giao thức mạng, dịch vụ mặc định không sử dụng cho dịch vụ.				
Có phương án cập nhật bản nâng cấp, bản vá lỗi của hệ điều hành và các	Đã có phương án định kỳ cập nhật bản vá hệ điều hành tối thiểu 3 tháng 1 lần.	Có phương án khả thi.				

dịch vụ đi kèm máy chủ, thiết bị.						
Máy chủ cài đặt phần mềm diệt Virus, phần mềm phòng chống mã độc hại.	Đã cài đặt phần mềm diệt virus có bản quyền và thường xuyên cập nhật bản phiên bản.	Có cài đặt phần mềm diệt virus đủ mạnh.				
Có chính sách định kỳ dò quét và xử lý phần mềm độc hại, điểm yếu ATTT.	Đã có quy trình, quy định định kỳ 6 tháng 1 lần dò quét và xử lý phần mềm độc hại, điểm yếu ATTT (đã được chứng nhận bởi một tổ chức có giấy phép kinh doanh dịch vụ ATTT). Hoặc thuê 1 tổ chức thứ 3 có giấy phép kinh doanh dịch vụ ATTT giám sát an toàn hệ thống.	Có quy trình, quy định dò quét và xử lý				
Máy chủ cài đặt phần mềm có bản quyền (OS, DB)	Đã có bản quyền (nếu phần mềm mất phí) cho Hệ quản trị CSDL.					
	Đã có bản quyền (nếu phần mềm mất phí) cho hệ điều hành.	Có bản quyền của Hệ điều hành và các phần mềm sử dụng trên hệ thống.				
4. Xử lý máy chủ, thiết bị khi chuyển giao mục đích sử dụng						
Có phương án xóa dữ liệu khi không còn sử	Đã có quy trình chính sách về việc xóa dữ liệu đảm bảo	Có quy trình, quy định xử lý thiết bị khi chuyển giao				

dụng. Đảm bảo dữ liệu không thể phục hồi sau khi xóa.	không thể khôi phục sau khi xóa.	hoặc hủy bỏ.				
	Sử dụng phần mềm chuyên dụng					
	Sử dụng phá hủy vật lý					
	Sử dụng định dạng nhiều lần					
	Sử dụng Phương pháp khác					

5.3 Mẫu đánh giá Phần mềm, ứng dụng

MẪU ĐÁNH GIÁ PHẦN MỀM, ỨNG DỤNG (Các yêu cầu bắt buộc)						
TCKT	**Bài đo và kết quả**					
	Các chỉ tiêu	**Kết quả mong muốn**	**Thực tế**	**Có**	**Không**	**Kết luận**
1.Xác thực, kiểm soát truy cập						
Lưu trữ mã hóa các thông tin nhạy cảm.	Mật khẩu đã phải được mã hóa khi lưu trữ.	Các thông tin nhạy cảm phải được mã hóa trong CSDL.				
	Bản dự phòng CSDL đã được mã hóa.					
Đảm bảo an toàn mật khẩu người sử dụng gồm: - Thay đổi mật khẩu mặc định - Sử dụng mật khẩu	Đã có chính sách mật khẩu phải bao gồm chữ hoa, chữ thường, ký tự đặc biệt và dài hơn 8 ký tự.	Có áp dụng chính sách mật khẩu mạnh.				
	Đã thiết lập chính sách bắt buộc 3 tháng thay đổi mật khẩu một lần.					

mạnh - Thiết lập thời gian thay đổi mật khẩu. - Số lần nhập sai mật khẩu	Đã thiết lập số lần nhập sai mật khẩu 5 lần sẽ bị khóa tài khoản.					
Thiết lập thời gian ngắt kết nối khi không có yêu cầu từ người dùng.	Đã giới hạn thời gian ngắt kết nối khi không có thao tác (Không quá 5 phút).	Ứng dụng có thiết lập thông số thời gian ngắt kết nối.				
Thiết lập phân quyền người dùng mức dữ liệu.	Kiểm tra về mặt chính sách phân quyền người dùng theo giải pháp.	Ứng dụng có phân quyền mức dữ liệu.				
2. Nhật ký hệ thống						
Ghi, lưu trữ nhật ký hệ thống trong thời gian tối thiểu 03 tháng, với các thông tin cơ bản sau: - Thông tin truy cập ứng dụng - Lỗi phát sinh hệ thống - Thông tin tác động, cấu hình từ quản trị viên	Tồn tại log nghiệp vụ từ trước lúc kiểm tra 3 tháng.	Ứng dụng có đầy đủ các Log tác động.				
	Tồn tại Log tác động cấu hình từ quản trị viên từ trước lúc kiểm tra 3 tháng.					
	Tồn tại log truy cập người dùng từ trước lúc kiểm tra 3 tháng.					

Nhật ký về các tác động lập, sửa, xóa, hủy hóa đơn điện tử phải được lưu trữ trong thời gian tối thiểu 10 năm kể từ thời điểm thực hiện thành công giao dịch	Đã có giải pháp lưu trữ log nghiệp vụ tối thiểu 10 năm an toàn và toàn vẹn.	Có ghi nhật ký và đơn vị được đánh giá chứng minh khả năng lưu trữ tối thiểu 10 năm.				
3. An toàn ứng dụng và mã nguồn, bảo mật dữ liệu						
Mã hóa các thông tin nhạy cảm, bí mật khi lưu trữ, khi truyền thông tin qua các kênh kết nối.	Đã mã hóa thông tin mật khẩu khi lưu trữ trong CSDL.	Ứng dụng có mã hóa thông tin nhạy cảm.				
	Đã sử dụng các giao thức an toàn: HTTPS hoặc TLS v2					
	Đã mã hóa dữ liệu dự phòng đảm bảo lưu trữ an toàn và toàn vẹn chưa.					
Có phương án bảo vệ ứng dụng chống lại các tấn công phổ biến như: SQL Injection, OS Command injection, XSS, CSRF, RFI, LFI, Xpath injection.	Đã có phương án bảo vệ ứng dụng chống lại các loại tấn công phổ biến như: SQL Injection, OS Command injection, XSS, CSRF, RFI, LFI, Xpath injection và đã được đánh giá (pentest).	Ứng dụng khắc phục các lỗ hổng trên.				
		Hệ thống phải được trang bị giải pháp bảo vệ như tường lửa ứng dụng.				

Có chức năng thông báo lỗi cho người dùng.	Ứng dụng đã có chức năng thông báo lỗi người dùng qua web					
	Ứng dụng đã có chức năng thông báo lỗi người dùng qua SMS					
	Ứng dụng đã có chức năng thông báo lỗi người dùng qua email	Có thông báo thông tin lỗi.				
Sử dụng chữ ký số để chống chối bỏ, xác thực các dữ liệu, thông tin quan trọng theo quy định. Chức năng ký số và xác thực ký số thực hiện theo đúng tiêu chuẩn tại Thông tư số 06/2015/TT-BTTTT ngày 23/03/2015.	Đã sử dụng chữ ký số để xác thực các thông tin quan trọng: Hóa đơn điện tử	Áp dụng đúng các thuật toán, thư viện SHA, RSA.				
	Chữ ký số trên hóa đơn đã tuân theo đúng tiêu chuẩn tại Thông tư số 06/2015/TT-BTTTT ngày 23/03/2015, Nghị Định 130/2018/NĐ-CP ngày 27/9/2018					
3. Sao lưu dự phòng, bảo đảm an toàn dữ liệu						

Có chính sách sao lưu dự phòng dữ liệu, log tác động, hệ điều hành định kỳ.	Đã có chính sách sao lưu dữ liệu, log tác động, hệ điều hành định kỳ (Thời gian lưu trữ, phương án lưu trữ đảm bảo an toàn và toàn vẹn).	Có chính sách sao lưu dữ liệu.				
	Đã có phương án đồng bộ dữ liệu giữa hệ thống chính và hệ thống dự phòng phải đồng bộ thời gian thực đảm bảo dữ liệu giữa 2 hệ thống luôn đầy đủ.					
Đường internet: Đường chính và đường dự phòng tối thiểu 10MB	Đã có tối thiểu 2 đường truyền phải của 2 nhà cung cấp khác nhau băng thông tối thiểu mỗi đường truyền 10MB.	Có tối thiểu 2 đường truyền có tốc độ theo quy định.				
Thiết bị lữu trữ Chứng thư số: thiết bị USB Token, HSM hoặc các thiết bị tương đương đảm bảo tiêu chuẩn của nhà nước (Nghị Định 130/2018/NĐ-CP, TT06/2015/TT-BTTTT).	Thiết bị lưu trữ chứng thư số khối an ninh phần cứng FIPS PUB 140-2 tối thiểu level 3.					
	Thiết bị lưu trữ thẻ Token và Smart card FIPS PUB 140-2 tối thiểu level 2.					

	Thiết bị lưu trữ chứng thư số khác.	Có lưu trữ chứng thư số trên HSM hoặc thiết bị tương đương.				
Hệ thống tường lửa, IPS/IDS Có khả năng phát hiện, cảnh báo và ngăn chặn các truy cập bất hợp pháp, các hình thức tấn công trên môi trường mạng.	Hệ thống tường lửa, IPS/IDS Có khả năng phát hiện, cảnh báo và ngăn chặn các truy cập bất hợp pháp, các hình thức tấn công trên môi trường mạng.	Có hệ thống Tường lửa và IPS/IDS tương đương phát hiện được tấn công dò quét khi thử nghiệm.				
Hệ thống máy chủ cài đặt theo công nghệ cluster, load balancing, quản trị từ xa. Có cán bộ trực hệ thống 24/7. Có điện thoại hỗ trợ KH.	Đã cài đặt công nghệ cluster	- Server có dự phòng - Có hệ thống lưu trữ dữ liệu đủ thời gian tối thiểu 10 năm - Có nhân sự trực 24/7				
	Đã cài đặt công nghệ load balancing					
	Đã phân công công cán bộ trực hệ thống 24/7					
	Đã có số điện thoại hỗ trợ khách hàng online 24/7					
Hệ thống UPS, hệ thống máy phát điện đảm bảo	Kiểm tra đánh giá tài liệu kỹ thuật mô tả hệ thống điện dự phòng.	Hệ thống UPS hoạt động online: Khi ngắt điện hệ thống UPS hoạt động và				

hoạt động hệ thống 24/7	Đã lắp đặt hệ thống UPS	kích hoạt máy phát điện hoạt động.				
	Đã có hệ thống máy phát điện dự phòng		d			
	Đã có chính sách và nhật ký thực tế việc bảo dưỡng UPS và hệ thống điện dự phòng đảm bảo hệ thống này hoạt động bình thường.					

5.4 Mẫu đánh giá an toàn thông tin vật lý

MẪU ĐÁNH GIÁ NHÂN SỰ VÀ TIÊU CHÍ KHÁC (Các yêu cầu bắt buộc)						
TCKT	**Bài đo và kết quả**					
	Các chỉ tiêu	**Kết quả mong muốn**	**Thực tế**	**Có**	**Không**	**Kết luận**
Có hệ thống camera an ninh giám sát phòng máy	Đã lắp đặt hệ thống camera an ninh cho hệ thống chính và hệ thống dự phòng.	- Có hệ thống Camera hoạt động tốt. - Có khả năng xem lại dữ liệu trong vòng tối thiểu 1 tháng từ ngày kiểm tra.				
	Đã lưu trữ dữ liệu của Camera đủ tối thiểu 1 tháng tính từ ngày kiểm tra					
Có các phương án và hệ thống dự phòng đảm bảo duy trì hoạt động an toàn, liên tục và có các phương án xử lý tình huống bất thường, khắc phục sự cố: quy trình phục hồi dữ liệu khi gặp sự cố; thời gian phục hồi dữ liệu tối đa 08 giờ kể	Đã có hệ thống dự phòng thảm họa đảm bảo khoảng cách tối thiểu 20 Km so với hệ thống chính Đã ban hành quy trình xử lý sự cố chưa?	- Có quy trình văn bản hóa - Thử nghiệm một quy trình thực tế để đảm bảo quy trình phù hợp và có hiệu lực				

từ thời điểm hệ thống gặp sự cố.						
Các yêu cầu đảm bảo an toàn PCCC: Có hệ thống báo cháy, báo nổ, chống sét, có hệ thống điều hòa tập trung.	Đã có hệ thống báo cháy, báo nổ	- Có hệ thống báo cháy, báo khói - Có hệ thống điều hòa tập trung… còn hoạt động bình thường				
	Đã có hệ thống điều hòa riêng và tập trung					
	Đã có chính sách định kỳ kiểm tra hệ thống có hoạt động bình thường không?					
Có hệ thống dự phòng thảm họa (DR) đặt cách xa hệ thống chính 20Km.	Đã có hệ thống dự phòng thảm họa đảm bảo khoảng cách tối thiểu 20Km so với hệ thống chính.	Có hệ thống dự phòng thảm họa với các tính năng đầy đủ như hệ thống chính				

5.5 Mẫu đánh giá tổ chức, nhân sự và các tiêu chí khác

MẪU ĐÁNH GIÁ NHÂN SỰ VÀ TIÊU CHÍ KHÁC (Các yêu cầu bắt buộc)						
TCKT	**Bài đo và kết quả**					
	Các chỉ tiêu	**Kết quả mong muốn**	**Thực tế**	**Có**	**Không**	**Kết luận**
1. Tổ chức						
Có tối thiểu 05 năm hoạt động trong lĩnh vực công nghệ thông tin.	Có giấy phép đăng ký kinh doanh	Căn cứ theo thời gian giấy phép đăng ký kinh doanh.				
Đã triển khai hệ thống, ứng dụng công nghệ thông tin cho tối thiểu 10 tổ chức	Đã có hợp đồng cung cấp dịch vụ.	Căn cứ theo hợp đồng của tổ chức.				
Có cam kết bảo lãnh của tổ chức tín dụng hoạt động hợp pháp tại Việt Nam với giá trị trên 5 tỷ đồng để giải quyết các rủi ro và bồi thường thiệt hại có thể xảy ra trong quá trình cung cấp dịch vụ	Đã có cam kết bảo lãnh.	Cung cấp giấy bảo lãnh ngân hàng còn hiệu lực.				

2. Nhân sự						
Có tối thiểu 20 cán bộ kỹ thuật trình độ đại học chuyên ngành về công nghệ thông tin.	Bằng cấp, chứng nhận hợp lệ	Cung cấp bằng cấp hợp lệ				
Cán bộ phụ trách ATTT phải có trình độ đại học, chuyên ngành CNTT, an toàn thông tin phù hợp với vị trí tuyển dụng.	Tối thiểu phải có 01 cán bộ phụ trách được đào tạo về ATTT (có bằng đại học chuyên ngành ATTT hoặc chứng chỉ về ATTT như CEH, Sec+ hoặc ECSA, LPT,… hoặc tương đương) và có kinh nghiệm làm việc tối thiểu 2 năm trong lĩnh vực ATTT .	Cung cấp bằng cấp, chứng nhận hợp lệ				
Cán bộ phụ trách quản trị mạng phải có trình độ đại học, chuyên ngành CNTT	Tối thiểu phải có 1 cán bộ phụ trách quản trị mạng có chứng chỉ quản trị mạng (CCNA, MCSA, CEH… hoặc tương đương).	Cung cấp bằng cấp, chứng nhận hợp lệ				
Có quy định, quy trình đảm bảo ATTT liên quan tới hệ thống cung cấp dịch vụ HĐĐT của đơn vị.	Có văn bản ban hành quy định	Quy định, quy trình.				

Cán bộ kỹ thuật có cam kết giữ bí mật thông tin liên quan tới tổ chức sau khi nghỉ việc.	Đã có cam kết giữ bí mật thông tin khi kết thúc hợp đồng.	Căn cứ theo hợp đồng, quy định của tổ chức.				
3. Các tiêu chí khác						
Thời gian dừng hệ thống để bảo trì không quá 2% tổng số giờ cung cấp dịch vụ;	Kiểm tra đánh giá quy trình xử lý sự cố.	Thời gian dừng hệ thống trong nhật ký <=2% thời gian hoạt động				
	Kiểm tra thực tế nhật ký các báo cáo sự cố và thời gian khắc phục, thông báo cho khách hàng.					