Phụ lục Ch.07
CÁC LOẠI RỦI RO ĐƯỢC NHẬN DIỆN TRONG QUY TRÌNH

A. Nhận ra điểm yếu – mối đe dọa

Nhận ra điểm yếu và mối đe dọa là điều phải làm trước tiên:

- Ôn lại Chương 2 - Mối đe dọa, Điểm yếu, Các mục tiêu kiểm soát và kiểm soát Rủi ro ATTT.
- Xem lại Bài tập Nhóm Chương 2.

B. Các loại rủi ro thường được nhận diện trong quy trình

Bảng A.1

stt	Loại rủi ro	Định nghĩa
1.	**Rủi ro trong Xử lý công việc**	- Rủi ro xử lý công việc là rủi ro xảy ra tổn thất (không đạt mục tiêu đề ra khi thực hiện) do thiếu sót trong quá trình xử lý công việc tại Doanh nghiệp hoặc xử lý giao dịch với khách hàng hoặc giao dịch của Doanh nghiệp trên thị trường hoặc xảy ra do kiểm soát quy trình nội bộ không chặt chẽ. - Nguyên nhân dẫn đến rủi ro này có thể đến từ sai phạm của nhân viên, lỗi hệ thống CNTT, thiết kế quy trình xử lý chưa đầy đủ và có thiếu sót hoặc có lỗi…*(ví dụ: thiết kế quy trình, chốt kiểm soát hoặc hệ thống CNTT, nguồn lực dùng cho quy trình…)* phát sinh trong chuỗi các bước thực hiện (giao dịch) của quy trình (trước cam kết, cam kết, xử lý, quản lý/duy trì và kết thúc); cách tổ chức công việc chưa khoa học thiếu giám sát độc lập hoặc khách quan khi giao việc. - *Một số ví dụ về rủi ro xử lý công việc:* *a) Truyền đạt thông tin sai lệch cho đồng nghiệp/khách hàng;* *b) Lỗi nhập/ xuất dữ liệu;* *c) Không đáp ứng thời hạn hoặc trách nhiệm;* *d) Vận hành sai mô hình/hệ thống;* *e) Lỗi ghi chép sổ sách;* *f) Lỗi khi đối chiếu / soát xét thông tin;* *g) Thực hiện sai nhiệm vụ được giao;* *h) Không thực hiện bàn giao (ca làm việc, tài sản, công việc);* *i) Thất bại trong quản lý tài sản được giao quản lý;* *j) Kịch bản xử lý sự cố mạng LAN tại Doanh nghiệp không dùng được do không cập nhật hoặc do lỗi thời (lạc hậu)…*

2.	**Rủi ro Công nghệ Thông tin**	- Rủi ro công nghệ thông tin là rủi ro xảy ra tổn thất (có thể lượng hóa được) cho hệ thống công nghệ thông tin (CNTT) của doanh nghiệp. - Nguyên nhân của rủi ro này đến từ điểm yếu trong hạ tầng CNTT của doanh nghiệp bị tác nhân tấn công khai thác, doanh nghiệp còn nhiều hạn chế về công nghệ và năng lực xử lý xét trên các khía cạnh về năng lực quản lý tính toàn vẹn, khả năng kiểm soát và tính liên tục. Hơn nữa, rủi ro CNTT xuất phát từ việc thiếu chiến lược và chính sách CNTT, và từ việc sử dụng CNTT kém hiệu quả. - *Một số ví dụ về rủi ro CNTT:* *a) Sử dụng công nghệ cũ;* *b) Phần cứng/phần mềm không được kiểm định, đánh giá đầy đủ;* *c) Hệ thống có độ phức tạp cao, phụ thuộc nhiều vào các nhân viên chủ chốt nội bộ và bên ngoài Doanh nghiệp;* *d) Quản lý sự thay đổi đối với các hoạt động hàng ngày hoặc với các dự án liên quan đến công nghệ không được chặt chẽ;* *e) Hành động truy cập trái phép vào tài khoản;* *f) Hệ thống CNTT vận hành không ổn định, ảnh hưởng đến giao dịch khách hàng (ví dụ máy chủ e-mail thường xuyên gặp sự cố, không gửi-nhận được thư khiến Doanh nghiệp và khách hàng không thể liên lạc và trao đổi thông tin)…*
3.	**Rủi ro An toàn Thông tin**	- Rủi ro An toàn thông tin (hay rủi ro bảo mật) khi 3 trụ cột CIA *("confidentiality, integrity and availability")* của thông tin bị tổn hại. - Rủi ro an toàn thông tin xảy ra khi Doanh nghiệp không đáp ứng một phần hoặc tất cả các Yêu cầu ATTT theo Tiêu chuẩn ISO 27001. - Rủi ro an toàn thông tin là rủi ro xảy ra tổn thất hoặc gây mất mát cho doanh nghiệp vì thông tin mật của doanh nghiệp bị rò rỉ ra bên ngoài, dẫn đến không đảm bảo tính toàn vẹn của dữ liệu. Các thông tin này có thể được lưu trữ, in ấn, hoặc truyền đạt dưới dạng vật lý/ điện tử. - Rủi ro an toàn thông tin xảy ra bởi nhiều nguyên nhân, có thể do nhân viên của doanh nghiệp, do người bên ngoài, do hệ thống CNTT, hoặc do thiết kế quy trình không đầy đủ (ví dụ: các quy định, các chốt kiểm soát, hệ thống CNTT chứa các nội dung quan trọng của Doanh nghiệp), và các nguyên nhân khách quan khác. - *Một số ví dụ về rủi ro ATTT:* *a) Không đáp ứng yêu cầu và biện pháp kiểm soát theo ISO 27001;* *b) Rủi ro có thể gây tổn hại đến tính bảo mật của thông tin (như hacker truy cập được vào cơ sở dữ liệu khách hàng…);* *c) Rủi ro có thể gây tổn hại đến tính toàn vẹn của thông tin (như dữ liệu bị điều chỉnh hay sửa chữa ngoài sự hiểu biết của Doanh nghiệp…) ;* *d) Rủi ro có thể gây tổn hại đến tính sẵn có của thông tin (như mã độc Ransomware mã hóa dữ liệu của tổ chức / cá nhân khiến họ không thể làm việc được với dữ liệu…;* *e) Đọc tài liệu trái phép; trộm cắp, gián điệp, điều chỉnh thông tin trái phép; gây gián đoạn thông tin; xử lý thông tin không đúng cách, truyền thông tin không đúng cách; hủy thông tin trái phép/ không đúng cách; tổn hại do tin tặc;…*

4.	**Rủi ro Kinh doanh Liên tục**	- Rủi ro Kinh doanh Liên tục là rủi ro xảy ra tổn thất do các hoạt kinh doanh hàng ngày của Doanh nghiệp bị gián đoạn. - Xét theo các yêu cầu trong tiêu chuẩn ISO 22301:2019 thì rủi ro kinh doanh liên tục là rủi ro xảy ra cho doanh nghiệp do không đáp ứng một phần hoặc toàn bộ các yêu cầu của tiêu chuẩn dẫn đến gián đoạn hoạt động kinh doanh hàng ngày của doanh nghiệp khi gặp sự cố. - Nguyên nhân dẫn đến việc gián đoạn kinh doanh này là: (a) các hành vi cố ý như phá hoại, khủng bố, đe dọa đánh bom, đình công, bạo loạn và tấn công nhân viên Doanh nghiệp; (b) thiên tai: mưa bão, bão tuyết, lũ lụt và động đất; hoặc (c) các sự cố không lường trước khác như: tai nạn, cháy nổ, mất điện, dịch bệnh và bất ổn chính trị. - Sự gián đoạn này có thể dẫn đến việc nhân viên không tiếp cận được chỗ làm hoặc nhân viên không có khả năng thực hiện các công việc hằng ngày của họ do không thể tiếp cận được chỗ làm việc thường ngày hoặc do tổn thất về cơ sở hạ tầng CNTT, các ứng dụng kinh doanh, hoặc cơ sở vật chất. - *Một số ví dụ về rủi ro kinh doanh liên tục:* *a) Mất điện/ gián đoạn cung cấp tiện ích;* *b) Ngừng hoạt động một thời gian theo quy định chung để chấp hành chỉ thị của Chính Phủ trong thời gian có dịch viêm phổi (Covid-19) xảy ra…*
5.	**Rủi ro Ủy thác**	- Rủi ro xảy ra do không vì lợi ích tốt nhất của khách hàng khi tư vấn, đầu tư phải chịu trách nhiệm giải trình hoặc bảo quản tài sản của khách hàng; không ngăn chặn, phát hiện hoặc khắc phục các sơ suất/vi phạm về trách nhiệm ủy thác; không giải quyết thỏa đáng các xung đột lợi ích có thể phát sinh. - Với tư cách là đơn vị nhận ủy thác, nhân viên Doanh nghiệp có nghĩa vụ tuân thủ nghiêm ngặt các tiêu chuẩn đạo đức và làm việc một cách chuyên nghiệp thận trọng, đồng thời đảm bảo phù hợp với pháp luật, các quy định và thỏa thuận hợp đồng. Rủi ro ủy thác xảy ra khi nhân viên Doanh nghiệp không tuân thủ nghĩa vụ như trên. - *Một số ví dụ về rủi ro ủy thác:* *a) Tư vấn cho khách hàng các biện pháp bảo mật dữ liệu (hay thông tin) không hiệu quả;* *b) Không bảo mật thông tin cho khách hàng (cố ý hay vô ý);* *c) Doanh nghiệp kinh doanh dịch vụ cho thuê không gian trên máy chủ (Server) để lưu trữ, xử lý dữ liệu…nhưng Doanh nghiệp đã không có các biện pháp hữu hiệu để giảm thiểu rủi ro cho khách hàng khi xảy ra tấn công mạng…*
6.	**Rủi ro**	- Rủi ro ghi nhận và báo cáo là rủi ro xảy ra do những sai sót trong khi ghi nhận sự việc / báo cáo (cho mục đích kiểm soát nội bộ hoặc công bố thông tin ra bên ngoài) dẫn đến tổn thất cho Doanh nghiệp hoặc cho khách hàng hoặc nhà đầu tư. Các ghi nhận sai trong sổ sách hoặc báo cáo của Doanh nghiệp có thể dẫn đến sai lệch trong báo cáo hiệu quả hoạt động của Doanh nghiệp.

	Ghi nhận và Báo cáo	- Rủi ro ghi nhận và báo cáo có thể phát sinh từ một hệ thống thông tin không có khả năng theo dõi và ghị nhận các hoạt động theo thời gian thực trên hệ thống. - *Một số ví dụ về Rủi ro Ghi nhận và Báo cáo:* *a) Ghi nhận sai số lượng/giá trị tài sản hoặc giá trị công nợ;* *b) Không tuân thủ hướng dẫn trong quy trình/quy định tại Doanh nghiệp; hướng dẫn của cơ quan kiểm toán / cơ quan thuế/…khi ghi nhận kết quả hoạt động hoặc sự việc phát sinh;* *c) Không thực hiện nghĩa vụ báo cáo bắt buộc;* *d) Báo cáo ra bên ngoài không phù hợp (phát sinh tổn thất)…*
7.	**Rủi ro Nhân sự**	- Rủi ro nhân sự thường có nguyên nhân từ sự yếu kém trong năng lực nhận thức và trách nhiệm của người lao động lảm việc tại doanh nghiệp. - Rủi ro nhân sự xảy ra do thiếu sót trong các quy trình và thủ tục liên quan đến việc tuyển dụng, quản lý, đánh giá năng lực, phân công lao động và đãi ngộ các nhân viên của doanh nghiệp mà trực tiếp gây ra tổn thất hoặc gián tiếp góp phần tạo ra các sự kiện thuộc các loại rủi ro khác dẫn đến tổn thất *(ví dụ: không đủ năng lực/trình độ, các nhân tài nghỉ việc,...).* - Các quy trình chính liên quan đến nhân sự bao gồm cung cấp nguồn lực, nghỉ việc, đào tạo và phát triển, lương thưởng, phúc lợi và quan hệ giữa các nhân viên không được thiết kế và ban hành đầy đủ hoặc có thiếu sót hoặc không tuân thủ hợp đồng lao động đã ký. - *Một số ví dụ về rủi ro nhân sự:* *a) Nhân viên bất mãn, làm việc bất cẩn, vi phạm quy định…;* *b) Phân biệt đối xử với người lao động;* *c) Vi phạm thông lệ làm việc và an toàn nơi làm việc;* *d) Môi trường và điều kiện làm việc không phù hợp với sức khỏe nhân viên và các trường hợp quy định an toàn lao động;* *e) Bồi thường tai nạn lao động;* *f) Nhân sự quan trọng của Doanh nghiệp trong dự án quan trọng (ví dụ dự án trí tuệ nhân tạo) bị sa thải hoặc bỏ việc do chính sách đãi ngộ không thỏa đáng khi dự án bị đình trệ khiến rủi ro chậm tiến độ giao hàng đã xảy ra…*
8.	**Rủi ro Tuân thủ**	- Rủi ro pháp lý là rủi ro các hoạt động của Doanh nghiệp không tuân thủ theo tất cả các Luật, các Quy định có liên quan của Cơ quan quản lý Nhà nước hiện hành. - Rủi ro pháp lý xảy ra khi các Hợp đồng (dịch vụ, mua bán, tư vấn…) của doanh nghiệp với khách hàng không được rà soát bởi cán bộ kiểm soát và khi cần, không được bộ phận pháp lý phê duyệt trước khi ký kết, bao gồm đánh giá tính đầy đủ và khả năng thực thi của hợp đồng. - Rủi ro pháp lý xảy ra khi doanh nghiệp không đáp ứng nghĩa vụ quy định trong Hợp đồng. - Rủi ro tuân thủ là rủi ro mà doanh nghiệp có khả năng bị áp dụng các hình phạt theo quy định của pháp luật *(ví dụ như bị giới hạn hoạt động kinh doanh hoặc bị yêu cầu báo cáo nhiều hơn)*, hoặc doanh nghiệp có khả năng bị thiệt hại về tài chính và/hoặc tổn hại danh tiếng do không tuân thủ đầy đủ các quy định của pháp luật hiện hành.

	và Pháp lý	- *Một số ví dụ về rủi ro tuân thủ và pháp lý:* *a) Vi phạm hướng dẫn (cố ý) của cơ quan quản lý / pháp luật;* *b) Vi phạm quy định bảo mật (theo luật pháp);* *c) Lạm dụng thông tin tuyệt mật;* *d) Doanh nghiệp cung cấp ra thị trường các sản phẩm CNTT thuộc diện quốc phòng nhưng lại không có giấy phép kinh doanh loại sản phẩm này…*
9.	**Rủi ro Nhà cung cấp**	- Rủi ro nhà cung cấp xảy ra khi các thỏa thuận hoạt động thuê ngoài và thỏa thuận khung tiêu chuẩn không được thực hiện với các nhà cung cấp chất lượng, được phê duyệt và chứng nhận; bên cạnh đó rủi ro này xảy ra là do các sản phẩm/dịch vụ bàn giao không phù hợp với nội dung hợp đồng hoặc không đáp ứng được các tiêu chuẩn chất lượng đã thỏa thuận. - *Một số ví dụ về rủi ro nhà cung cấp:* *a) Thuê ngoài (không có hợp đồng, không ràng buộc nghĩa vụ…);* *b) Tranh chấp với nhà cung cấp;* *c) Các tổn thất phát sinh từ thất bại trong việc thực hiện, bàn giao, nghiệm thu và quản lý quy trình khác;* d) *Quá trình đấu thầu chọn nhà cung cấp không có năng lực do đã không thực hiện đấu thầu rộng rãi, công khai mà lại tiết lộ yêu cầu của chủ đầu tư chỉ cho một nhà cung cấp quen thân với nhóm lợi ích trong Doanh nghiệp…*
10.	**Rủi ro Nhận biết khách hàng**	- Rủi ro nhận biết khách hàng là các rủi ro phát sinh khi Doanh nghiệp không biết đầy đủ về khách hàng nhưng lại ký hợp đồng giao dịch với khách hàng hoặc không thực hiện giám sát giao dịch để xác định và phát hiện các hoạt động đáng ngờ và không báo cáo hoạt động đáng ngờ kịp thời và chính xác cho lãnh đạo Doanh nghiệp và các cơ quan pháp luật. - Để tránh rủi ro này Doanh nghiệp phải thực hiện một quá trình thẩm định khách hàng trước khi ký hợp đồng giao dịch để đánh giá rủi ro và kiểm soát pháp lý đối với khách hàng của họ. - *Một số ví dụ về Rủi ro nhận biết khách hàng:* *a) Ký hợp đồng với khách hàng đã từng vi phạm bảo mật thông tin;* *b) Giao dịch với khách hàng có quan hệ với đối thủ cạnh tranh;* *c) Mua hàng hóa công nghệ của khách nhưng không tìm hiểu kỹ nguồn gốc của hàng hóa đó;* *d) Doanh nghiệp đã ký hợp đồng mua hàng công nghệ với một tổ chức không có chức năng kinh doanh loại hàng hóa đó; hoặc Doanh nghiệp cho tổ chức vay tiền triển khai dự án CNTT nhưng không thẩm định chính xác năng lực nghiên cứu và phát triển của tổ chức đối với sản phẩm có chỉ định các điều kiện đặc biệt…*
11.	**Rủi ro**	- Rủi ro an ninh vật lý bao gồm rủi ro cơ sở hạ tầng, tài sản vật chất & rủi ro kiểm soát ra vào nơi làm việc. Rủi ro cơ sở hạ tầng là rủi ro làm phát sinh tổn thất do thiệt hại và/hoặc hư hỏng tài sản vật chất của Doanh nghiệp hoặc tổn thất về việc cung cấp dịch vụ của đối tác, có khả năng ảnh hưởng đến một hoặc nhiều Đơn vị kinh doanh hoặc dẫn đến sự gián đoạn của một số hoạt động chung (như công trình sử dụng chung, nước, điện) hoặc ảnh hưởng đến sự vận hành cơ sở hạ tầng tại trụ sở Doanh

	An ninh Vật lý (Cơ sở hạ tầng)	nghiệp (năng lượng, máy sưởi, thông gió, máy lạnh, thang máy và hệ thống phòng cháy chữa cháy), một số được phân loại là quan trọng. - *Một số ví dụ về Rủi ro an ninh vật lý (cơ sở hạ tầng):* *a) Không đáp ứng yêu cầu theo Điều A.11 ISO 27001;* *b) Xây dựng tòa nhà đặt phòng máy chủ trên nền đất yếu;* *c) Không có dự phòng khi đặt cáp truyền thông giữa các tòa nhà;* *d) Bồn dầu cho máy phát điện (máy phát điện đặt tại Doanh nghiệp để sử dụng khi mất điện lưới) có thiết kế không đáp ứng an toàn phòng cháy chữa cháy…*
12.	**Rủi ro An ninh**	- Rủi ro an ninh là rủi ro làm phát sinh tổn thất do các cuộc tấn công hoặc các hành động/sự cố/sự kiện gây thiệt hại đến: a) Con người bao gồm nhân viên Doanh nghiệp, khách hàng và nhà cung cấp – khi đang có mặt trụ sở Doanh nghiệp hoặc đi công tác; b) Tài sản của Doanh nghiệp bao gồm các trụ sở làm việc và cơ sở hạ tầng; c) Thông tin - được lưu trữ, in ấn, nói, truyền đi dưới dạng hồ sơ giấy/điện tử – do tổn thất, phá hủy, thay đổi tài sản hoặc phát hiện vô tình/cố ý. - Rủi ro an ninh bao gồm việc quản lý các tài sản (như máy vi tính, máy in, chứng khoán, tiền mặt,…) và quyền tiếp cận các trụ sở/khu vực nơi các tài sản giá trị, dễ di chuyển được cất giữ dưới hình thức tài sản bảo đảm (chứng khoán, các giấy tờ có giá (dạng để trống), các công cụ chuyển đổi, các ghi nhận kế toán, hồ sơ pháp lý và các giấy tờ liên quan đến tài sản đảm bảo…). - *Một số ví dụ về rủi ro an ninh:* *a) Không đáp ứng yêu cầu theo Điều A.6, A.7, A.8, A.9, A.10, A.11, A.12, A.13,... ISO 27001;* *b) Gian lận trong giao dịch với khách hàng; hối lộ/đút lót;* *c) Ăn cắp/tống tiền/biển thủ/trộm cắp/phá hoại tài sản;* *d) Giả mạo chữ ký, giấy tờ; dùng thẻ giả để truy cập;* *e) Khủng bố, phá hoại, đe dọa đánh bom* *f) Tòa nhà Doanh nghiệp không có cửa ra vào kiên cố, không có trang bị máy ghi hình (camera) và các biện pháp kiểm soát ra vào (thẻ ra vào, ...) v.v khiến kẻ trộm có thể xâm nhập và chiếm đoạt bất hợp pháp tài sản của Doanh nghiệp*
13.	**Rủi ro**	- Rủi ro danh tiếng xảy ra khi kỳ vọng của các bên liên quan - chẳng hạn như khách hàng, nhân viên, nhà cung cấp bên thứ ba, nhà đầu tư và cơ quan quản lý - cao hơn thực tế mà Doanh nghiệp mang lại hoặc Doanh nghiệp đã không đáp ứng kỳ vọng của các bên liên quan. - Những loại rủi ro danh tiếng là: Hành vi kém của lãnh đạo Doanh nghiệp hoặc thậm chí là một nhân viên có giao tiếp với khách hàng; chất lượng

	về danh tiếng	dịch vụ và sản phẩm không phù hợp hoặc kém chất lượng; Doanh nghiệp không theo kịp niềm tin đang thay đổi của các bên liên quan…; - *Một số ví dụ về rủi ro về danh tiếng:* *a) Bị đánh cắp thông tin mật (do kẻ xấu, nhân viên bất mãn…làm)* *b) Từ chối bảo hành sản phẩm còn trong thời hạn bảo hành;* *c) Ứng xử thô lỗ, thiếu tôn trọng khách hàng;* *d) Từ chối bảo trì, sửa chữa hư hỏng của sản phẩm thuộc phạm vi trách nhiệm của mình…*
14.	**Rủi ro chiến lược**	- *"Chiến lược":* là từ chỉ các kế hoạch hành động được vạch ra để đạt được các mục tiêu chiến lược. Thời gian thực hiện chiến lược thường là từ 5 năm trở lên hoặc lâu hơn nhưng thời gian này có thể thay đổi vì phụ thuộc vào bối cảnh (bên trong và bên ngoài) hoạt động của doanh nghiệp. - Khi Doanh nghiệp cố gắng đạt được các mục tiêu chiến lược, nhưng các sự kiện bên trong và bên ngoài xảy ra có thể cản trở hoặc ngăn cản Doanh nghiệp hoàn thành các mục tiêu đó. Điều này được gọi là rủi ro chiến lược. - *Một số ví dụ về rủi ro chiến lược:* *a) Sản phẩm chính của Doanh nghiệp bị lỗi thời nhanh chóng;* *b) Loại hình kinh doanh chính của Doanh nghiệp không còn phù hợp với yêu cầu mới của thị trường;* *c) Mục tiêu chiến lược của Doanh nghiệp là trở thành nhà cung cấp dịch vụ hàng đầu về AI (trí tuệ nhân tạo) vào năm 2025 nhưng người lãnh đạo cao nhất của Doanh nghiệp lại bị các cổ đông sa thải vì quan điểm kinh doanh không phù hợp dẫn đến sự ra đi hàng loạt nhân tài AT của Doanh nghiệp. Rủi ro này được xem như là rủi ro chiến lược của Doanh nghiệp….*
15.	**Rủi ro Khác**	- Các rủi ro không xếp vào các loại rủi ro liệt kê như trên - Các rủi ro khi Doanh nghiệp không đáp ứng bộ yêu cầu của ISO 27001 nhưng không hiện diện trong các bước của quy trình.

C. Áp dụng

1. Quy trình Khắc phục sự cố hệ thống Mạng nội bộ (LAN) tại công ty

Xem nội dung trong tập tin ***BaiTap_Ch.07_PhantichQuytrinh_Apdung-FMEA_ng11042025.xlsx***

2. Nhận diện rủi ro tiềm ẩn cho Quy trình khi phân tích rủi ro có sử dụng Bảng A.1:

Sử dụng Bảng A.1 ở trên, đối chiếu 2 chiều với từng loại rủi ro khi nhận diện và phân tích rủi ro tiềm ẩn cho *"Quy trình Khắc phục sự cố hệ thống Mạng nội bộ (LAN) tại doanh nghiệp"*, các rủi ro sau đây đã được nhận diện và thuộc các LOẠI RỦI RO sau:

TT	Các bước thực hiện quy trình	Rủi ro tiềm ẩn được nhận diện	Xem xét trước Loại rủi ro tại Bảng A.1 để suy ra rủi ro tiềm ẩn hoặc ngược lại
1	*2*	*3*	*4*
1	Bước 1:	Hệ thống email có thể không hoạt động	Rủi ro Công nghệ Thông tin

TT	Các bước thực hiện quy trình	Rủi ro tiềm ẩn được nhận diện	Xem xét trước Loại rủi ro tại Bảng A.1 để suy ra rủi ro tiềm ẩn hoặc ngược lại
	Tiếp nhận thông tin sự cố		
2	Bước 2: Cập nhật sự cố vào sổ nhật ký	Nhân viên tổ vận hành PQLVH có thể quên / không ghi nhận sự cố vào sổ nhật ký	Rủi ro Xử lý công việc, và Rủi ro Ghi nhận và Báo cáo
3	Bước 3. Xác định nguyên nhân và cập nhật thông tin sự cố	Nhân viên tổ vận hành PQLVH có thể quên / không ghi nhận nguyên nhân sự cố vào sổ nhật ký	Rủi ro Xử lý công việc, và Rủi ro Ghi nhận và Báo cáo
4	Bước 4. Xác định có kịch bản khắc phục chưa?	Có kịch bản nhưng có thể kịch bản không thực thi được một số bước	Rủi ro Công nghệ Thông tin
5	Bước 5. Xây dựng phương án khắc phục	Có thể xác định sai nguyên nhân gây ra sự cố khi xây dựng phương án	Rủi ro nhân sự (do nhân sự được huấn luyện kém / tuyển dụng nhân viên có năng lực kém /…)
6	Bước 6. Phê duyệt	(1)Phương án có thể không được duyệt trên văn bản	Rủi ro Xử lý công việc
		(2)Phương án có thể không được duyệt trên văn bản đủ nhanh để kịp khắc phục sự cố trong thời gian quy định	Rủi ro Xử lý công việc, và Rủi ro Nhân sự
7	Bước 7. Khắc phục sự cố	Công cụ chuyên dụng dùng trong phương án xử lý (như kìm bấm RJ45, LAN cable tester,…) có thể bị hỏng hoặc thiếu hoặc thất lạc hoặc bị nhân viên mang đi nơi khác.	Rủi ro Xử lý công việc
8	Bước 8. Kiểm tra kết quả	Sự cố có thể vẫn chưa khắc phục xong	Rủi ro Nhân sự, và Rủi ro Xử lý công việc
9	Bước 9. Báo cáo - cập nhật thông tin sự cố	Nhân viên tổ vận hành PQLVH có thể cập nhật thiếu thông tin vào sổ nhật kí	Rủi ro Nhân sự, và Rủi ro Xử lý công việc Rủi ro Ghi nhận và Báo cáo
10	Bước 10. Lưu hồ sơ	Hồ sơ có thể không có Phiếu yêu cầu (tập tin số qua email) tại Bước 1 theo Quy định do hệ thống email không hoạt động trước-trong-và sau khi khắc phục sự cố mạng	Rủi ro CNTT, Rủi ro Nhân sự, Rủi ro Xử lý công việc, và Rủi ro Ghi nhận và Báo cáo

./.