BỘ THÔNG TIN VÀ TRUYỀN THÔNG

CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
Độc lập - Tự do - Hạnh phúc

Số: 17 /2021/TT-BTTTT

Hà Nội, ngày 30 tháng 11 năm 2021

THÔNG TƯ

Sửa đổi, bổ sung một số điều Thông tư số 11/2015/TT-BTTTT ngày 05 tháng 5 năm 2015 của Bộ Thông tin và Truyền thông Quy định Chuẩn kỹ năng nhân lực công nghệ thông tin chuyên nghiệp

Căn cứ Luật Công nghệ thông tin ngày 29 tháng 6 năm 2006;

Căn cứ Luật An toàn thông tin mạng ngày 19 tháng 11 năm 2015;

Căn cứ Nghị định số 17/2017/NĐ-CP ngày 17 tháng 02 năm 2017 của Chính phủ quy định chức năng, nhiệm vụ, quyền hạn và cơ cấu tổ chức của Bộ Thông tin và Truyền thông;

Căn cứ Nghị định số 71/2007/NĐ-CP ngày 03 tháng 5 năm 2007 của Chính phủ quy định chi tiết và hướng dẫn thực hiện một số điều của Luật Công nghệ thông tin về Công nghiệp công nghệ thông tin;

Theo đề nghị của Cục trưởng Cục An toàn thông tin và Vụ trưởng Vụ Công nghệ thông tin;

Bộ trưởng Bộ Thông tin và Truyền thông ban hành Thông tư sửa đổi, bổ sung một số điều Thông tư số 11/2015/TT-BTTTT ngày 05 tháng 5 năm 2015 của Bộ Thông tin và Truyền thông Quy định Chuẩn kỹ năng nhân lực công nghệ thông tin chuyên nghiệp.

Điều 1. Sửa đổi, bổ sung một số điều Thông tư số 11/2015/TT-BTTTT ngày 05 tháng 5 năm 2015 của Bộ Thông tin và Truyền thông Quy định Chuẩn kỹ năng nhân lực công nghệ thông tin chuyên nghiệp (sau đây gọi là Thông tư số 11/2015/TT-BTTTT), như sau:

1. Khoản 4 Điều 1 được sửa đổi, bổ sung như sau:

"4. Chuẩn kỹ năng An toàn thông tin (Cybersecurity Skill Standard);"

2. Khoản 1 Điều 3 được sửa đổi, bổ sung như sau:

"1. Các ngành đào tạo về công nghệ thông tin bao gồm: Khoa học máy

tính, Mạng máy tính và truyền thông dữ liệu, Kỹ thuật phần mềm, Hệ thống thông tin, Kỹ thuật máy tính, Công nghệ kỹ thuật máy tính, Công nghệ thông tin, An toàn thông tin, Kỹ thuật sửa chữa, lắp ráp máy tính, Thiết kế mạch điện tử trên máy tính, Truyền thông và mạng máy tính, Điện tử máy tính, Công nghệ truyền thông, Sư phạm Tin học, Tin học ứng dụng, Tin học viễn thông ứng dụng, Xử lý dữ liệu, Lập trình máy tính, Quản trị mạng máy tính, Quản trị hệ thống, Toán ứng dụng, Đảm bảo toán học cho máy tính và hệ thống tính toán, Điện tử tin học và các ngành thuộc nhóm ngành Máy tính và Công nghệ thông tin theo quy định của Bộ Giáo dục và Đào tạo tại Danh mục giáo dục đào tạo cấp IV - trình độ đại học và Danh mục ngành, nghề đào tạo cấp IV trình độ cao đẳng của Bộ Lao động - Thương binh và Xã hội;

3. Điểm d khoản 1 Điều 4 được sửa như sau:

"d) Chuẩn kỹ năng An toàn thông tin (Mã CSSS): là hệ thống các yêu cầu kiến thức và kỹ năng cần thiết để thực hiện những công việc liên quan đến an toàn thông tin."

4. Thay thế cụm từ "- Chuẩn kỹ năng An toàn thông tin: các yêu cầu về kiến thức, kỹ năng chuyên sâu của Chuẩn kỹ năng An toàn thông tin được quy định tại Phụ lục số 05 Thông tư này" bằng cụm từ "- Chuẩn kỹ năng An toàn thông tin: các yêu cầu về kiến thức, kỹ năng chuyên sâu của Chuẩn kỹ năng An toàn thông tin được quy định tại Phụ lục Thông tư này." tại điểm b khoản 2 Điều 4.

Điều 2. Thay thế Phụ lục số 05 Yêu cầu về kiến thức, kỹ năng chuyên sâu của Chuẩn kỹ năng An toàn thông tin tại Thông tư số 11/2015/TT-BTTTT bằng Phụ lục Yêu cầu về kiến thức, kỹ năng chuyên sâu của Chuẩn kỹ năng An toàn thông tin ban hành kèm theo Thông tư này.

Điều 3. Tổ chức thực hiện

1. Chánh Văn phòng, Cục trưởng Cục An toàn thông tin, Vụ trưởng Vụ Công nghệ thông tin, Thủ trưởng các cơ quan, đơn vị thuộc Bộ Thông tin và Truyền thông, Giám đốc Sở Thông tin và Truyền thông các tỉnh, thành phố trực thuộc Trung ương và các cơ quan, tổ chức, cá nhân có liên quan chịu trách nhiệm thi hành Thông tư này.

2. Giao Cục An toàn thông tin chủ trì, phối hợp Vụ Công nghệ thông tin tham mưu, hướng dẫn tổ chức thực hiện về Chuẩn kỹ năng An toàn thông tin.

Điều 4. Điều khoản thi hành

Thông tư này có hiệu lực thi hành kể từ ngày 01 tháng 6 năm 2022./.

Nơi nhận:
- Thủ tướng, các Phó Thủ tướng Chính phủ (để b/c);
- Văn phòng Chính phủ;
- Văn phòng Chủ tịch nước;
- Văn phòng Quốc hội;
- Văn phòng Trung ương Đảng và các Ban của Đảng;
- Văn phòng Tổng Bí thư;
- Các Bộ, cơ quan ngang Bộ, cơ quan thuộc Chính phủ;
- Toà án nhân dân tối cao;
- Viện Kiểm sát nhân dân tối cao;
- Kiểm toán Nhà nước;
- UBND các tỉnh, thành phố trực thuộc TW;
- Đơn vị chuyên trách về CNTT của các Bộ, cơ quan ngang Bộ, cơ quan thuộc Chính phủ;
- Sở Thông tin và Truyền thông các tỉnh, thành phố trực thuộc TW;
- Công báo, Cổng Thông tin điện tử Chính phủ;
- Cục Kiểm tra VBQPPL (Bộ Tư pháp);
- Bộ TTTT: Bộ trưởng và các Thứ trưởng, các cơ quan, đơn vị thuộc Bộ; Cổng Thông tin điện tử Bộ;
- Lưu: VT, CATTT.

BỘ TRƯỞNG

BỘ THÔNG TIN VÀ TRUYỀN THÔNG

Nguyễn Mạnh Hùng

Phụ lục

YÊU CẦU VỀ KIẾN THỨC, KỸ NĂNG CHUYÊN SÂU CỦA CHUẨN KỸ NĂNG AN TOÀN THÔNG TIN

(Ban hành kèm theo thông tư số 17/2021/TT-BTTTT ngày 30/11/2021 của Bộ trưởng Bộ Thông tin và Truyền thông)

Mã Tham chiếu	Mã Kiến thức	Kiến thức	Mã Kỹ năng	Kỹ năng	4	3	2	1
CSSS 1	**Quản lý rủi ro**					x	x	x
	KT001	Kiến thức về các khái niệm và giao thức mạng máy tính và phương pháp luận về an toàn thông tin mạng.	KN001	Kỹ năng tiến hành rà quét điểm yếu và nhận biết các điểm yếu để đảm bảo an toàn các hệ thống.				
	KT002	Kiến thức về các quy trình quản lý rủi ro (ví dụ: các phương pháp đánh giá và giảm thiểu rủi ro).	KN004	Kỹ năng áp dụng các nguyên tắc tính bí mật, tính toàn vẹn và tính sẵn sàng.				
	KT003	Kiến thức về luật, quy định, chính sách và đạo đức nghề nghiệp liên quan đến an toàn thông tin mạng và quyền riêng tư.	KN013	Kỹ năng xác định cách thức hoạt động của hệ thống bảo mật (bao gồm khả năng phục hồi và khả năng tin cậy) và những thay đổi về điều kiện, hoạt động hoặc môi trường sẽ ảnh hưởng như thế nào đến những kết quả này.				
	KT004	Kiến thức về an toàn thông tin mạng và các nguyên tắc quyền riêng tư.	KN016	Kỹ năng xác định nhu cầu bảo vệ (ví dụ: các kiểm soát an toàn) của hệ thống thông tin và mạng.				
	KT005	Kiến thức về các mối đe dọa và điểm yếu an toàn thông tin mạng.	KN018	Kỹ năng xác định các biện pháp hoặc chỉ số về hiệu suất của hệ thống và các hành động cần thiết để cải thiện hoặc hiệu chỉnh hiệu suất liên quan đến các mục tiêu của hệ thống.				
	KT006	Kiến thức về các ảnh hưởng đối với hoạt động do mất an toàn thông tin mạng.	KN038	Kỹ năng sử dụng máy ảo. (Ví dụ: Microsoft Hyper-V, VMWare, VirtualBox, v.v.).				

Mã Tham chiếu	Mã Kiến thức	Kiến thức	Mã Kỹ năng	Kỹ năng	4	3	2	1
	KT007	Kiến thức về phương pháp xác thực, ủy quyền và kiểm soát truy cập.	KN043	Kỹ năng nhận biết, phân loại các loại điểm yếu và các hình thức tấn công liên quan.				
	KT008	Kiến thức về áp dụng các quy trình kinh doanh và hoạt động của các tổ chức.	KN057	Kỹ năng áp dụng các kiểm soát an toàn.				
	KT009	Kiến thức về các điểm yếu ứng dụng.	KN058	Kỹ năng sử dụng hoặc phát triển các hoạt động học tập (ví dụ: kịch bản, hướng dẫn trò chơi, bài tập tương tác).				
	KT010	Kiến thức về các phương pháp kết nối, nguyên tắc và khái niệm hạ tầng mạng.	KN059	Kỹ năng xác định các yêu cầu Kiểm tra & Đánh giá hạ tầng (con người, phạm vi, công cụ, thiết bị đo đạc)				
	KT011	Kiến thức về khả năng và ứng dụng của thiết bị mạng bao gồm bộ định tuyến (router), thiết bị chuyển mạch (switch), cầu nối (bridge), máy chủ, phương tiện truyền dẫn và phần cứng liên quan.	KN060	Kỹ năng giao tiếp với khách hàng.				
	KT013	Kiến thức về các công cụ bảo vệ và đánh giá điểm yếu an toàn thông tin mạng và khả năng của các công cụ.	KN061	Kỹ năng quản lý tài sản kiểm tra, tài nguyên kiểm tra và nhân sự kiểm tra để đảm bảo hoàn thành các sự kiện kiểm tra một cách hiệu quả.				
	KT018	Kiến thức về mật mã và các khái niệm quản lý khóa mật mã.	KN062	Kỹ năng lập báo cáo kiểm tra, đánh giá.				
	KT017	Kiến thức về các thuật toán mã hóa.	KN064	Kỹ năng xem lại nhật ký để xác định bằng chứng về những lần xâm nhập trong quá khứ.				
	KT019	Kiến thức về sao lưu và phục hồi dữ liệu.	KN067	Kỹ năng xử lý sự cố và chẩn đoán các bất thường về hạ tầng bảo vệ mạng và cách giải quyết vấn đề.				
	KT020	Kiến thức về hệ thống cơ sở dữ liệu.	KN068	Kỹ năng sử dụng nhân lực và nhân sự hệ thống CNTT.				

Mã Tham chiếu	Mã Kiến thức	Kiến thức	Mã Kỹ năng	Kỹ năng	4	3	2	1
	KT021	Kiến thức về kế hoạch duy trì hoạt động và khôi phục thảm họa.	KN072	Kỹ năng rà soát lại, xem xét các hệ thống.				
	KT022	Kiến thức về kiến trúc an toàn thông tin của tổ chức.	KN073	Kỹ năng xây dựng kế hoạch kiểm thử an toàn thông tin (ví dụ: đơn vị, tích hợp, hệ thống, chấp nhận).				
	KT023	Kiến thức về các yêu cầu đánh giá và xác nhận của tổ chức.	KN074	Kỹ năng về các nguyên tắc, mô hình, phương pháp và các công cụ quản lý hệ thống mạng.				
	KT024	Kiến thức về kết nối Mạng cục bộ (LAN) và mạng diện rộng (WAN) của tổ chức.	KN075	Kỹ năng thực hiện đánh giá điểm yếu an toàn ứng dụng.				
	KT031	Kiến thức về quy trình Đánh giá và Ủy quyền bảo mật an toàn thông tin mạng.	KN076	Kỹ năng sử dụng mã hóa hạ tầng khóa công khai (PKI) và chữ ký số vào các ứng dụng (ví dụ: email S/MIME, SSL).				
	KT032	Kiến thức về các nguyên tắc an toàn thông tin mạng và riêng tư được sử dụng để quản lý rủi ro liên quan đến việc sử dụng, lưu trữ và truyền thông tin hoặc dữ liệu.	KN079	Kỹ năng đánh giá an toàn thiết kế hệ thống.				
	KT034	Kiến thức về các nguồn phổ biến thông tin về điểm yếu bảo mật (ví dụ: cảnh báo, tư vấn và bản tin,...).	KN080	Kỹ năng tích hợp và áp dụng các chính sách để đáp ứng các mục tiêu an toàn hệ thống.				
	KT038	Kiến thức về các nguyên tắc và yêu cầu an toàn thông tin mạng và riêng tư (liên quan đến tính bí mật, tính toàn vẹn, tính khả dụng, xác thực, chống chối bỏ).	KN081	Kỹ năng đánh giá các biện pháp kiểm soát an toàn dựa trên các nguyên tắc và nguyên lý an toàn thông tin mạng.				
	KT041	Kiến thức về các yêu cầu quản lý rủi ro.	KN090	Kỹ năng thực hiện đánh giá tác động/rủi ro.				

Mã Tham chiếu	Mã Kiến thức	Kiến thức	Mã Kỹ năng	Kỹ năng	4	3	2	1
	KT042	Kiến thức về các nguyên tắc và phương pháp an toàn thông tin (ví dụ: tường lửa, DMZ, mã hóa).	KN091	Kỹ năng áp dụng các kỹ thuật lập trình an toàn.				
	KT046	Kiến thức về các phương pháp chuyên ngành về thẩm định, triển khai và áp dụng đánh giá an toàn thông tin, giám sát, phát hiện; các công cụ và quy trình khắc phục theo các tiêu chuẩn.	KN092	Kỹ năng sử dụng các công cụ hiệu chỉnh tương quan sự kiện an toàn thông tin.				
	KT048	Kiến thức về truy cập mạng, danh tính và quản lý truy cập (ví dụ: hạ tầng khóa công khai, Oauth, OpenID, SAML, SPML).	KN093	Kỹ năng sử dụng các công cụ phân tích dòng lệnh (code).				
	KT051	Kiến thức về các công nghệ mới và mới nổi lĩnh vực công nghệ thông tin và an toàn thông tin mạng.	KN094	Kỹ năng thực hiện phân tích nguyên nhân gốc.				
	KT060	Kiến thức về các mối đe dọa và điểm yếu của hệ thống và ứng dụng (ví dụ: tràn bộ đệm (buffer overflow), mã di động (mobile code), cross-site scripting, PL/SQL injection, mã độc,...).	KN095	Kỹ năng trong các hoạt động lập kế hoạch hành chính.				
	KT071	Kiến thức về các nguyên tắc và phương pháp phân tích cấu trúc.	KN096	Kỹ năng phân tích mạng liên lạc của mục tiêu.				
	KT074	Kiến thức về các công cụ đánh giá hệ thống và kỹ thuật xác định lỗi.	KN097	Kỹ năng phân tích lưu lượng để xác định các thiết bị mạng.				
	KT079	Kiến thức về cấu trúc và quy trình báo cáo của nhà cung cấp dịch vụ an toàn thông tin mạng.	KN106	Kỹ năng xác định các thiếu sót và hạn chế của hoạt động thu thập thông tin.				
	KT080	Kiến thức về kiến trúc công nghệ thông tin, Chính phủ điện tử.	KN107	Kỹ năng xác định các ngôn ngữ vấn đề có thể tác động đến các mục tiêu của tổ chức.				
	KT081	Kiến thức về các tầm nhìn và mục tiêu công nghệ thông tin của tổ chức.	KN108	Kỹ năng xác định khách hàng tiềm năng để phát triển mục tiêu.				

Mã Tham chiếu	Mã Kiến thức	Kiến thức	Mã Kỹ năng	Kỹ năng	4	3	2	1
	KT099	Kiến thức về thực hành Quản lý rủi ro chuỗi cung ứng.	KN109	Kỹ năng xác định các ngôn ngữ và phương ngữ (thổ ngữ).				
	KT110	Kiến thức về các quy trình kinh doanh / sứ mệnh cốt lõi của tổ chức.	KN110	Kỹ năng xác định các thiết bị hoạt động ở mỗi tầng của các mô hình giao thức.				
	KT118	Kiến thức về luật, nghị định, chỉ thị, quy định hiện hành về an toàn thông tin.	KN111	Kỹ năng xác định, định vị và theo dõi mục tiêu thông qua các kỹ thuật phân tích không gian địa lý.				
	KT119	Kiến thức về an toàn chuỗi cung ứng công nghệ thông tin và rủi ro chuỗi cung ứng, các chính sách, yêu cầu và thủ tục quản lý.	KN112	Kỹ năng ưu tiên thông tin liên quan đến nghiệp vụ.				
	KT120	Kiến thức về các hệ thống hạ tầng quan trọng với công nghệ thông tin và truyền thông được thiết kế không quan tâm về bảo mật hệ thống.	KN113	Kỹ năng diễn giải các ngôn ngữ lập trình biên dịch và thông dịch.				
	KT127	Kiến thức về các khái niệm kiến trúc an toàn thông tin mạng bao gồm cấu trúc liên kết (topology), giao thức, các thành phần và nguyên tắc (ví dụ: phòng thủ chiều sâu defense-in-depth).	KN114	Kỹ năng diễn giải siêu dữ liệu và nội dung được áp dụng bởi hệ thống thu thập.				
	KT141	Kiến thức về các khái niệm kiến trúc an toàn thông tin và các kiến trúc mô hình tham chiếu (ví dụ: Khung kiến trúc Zachman, v.v.).	KN115	Kỹ năng diễn giải các kết quả truy vết, cũng như áp dụng cho việc phân tích và cấu trúc lại hệ thống mạng.				
	KT144	Kiến thức về các mô hình bảo mật (ví dụ: mô hình Bell-LaPadula, mô hình Biba, Mô hình Clark Wilson).	KN116	Kỹ năng giải thích kết quả rà quét điểm yếu để xác định điểm yếu.				
	KT162	Kiến thức về các tiêu chuẩn an toàn thông tin cá nhân, dữ liệu cá nhân.	KN117	Kỹ năng quản lý kiến thức, tài liệu kỹ thuật (ví dụ: Wikipage).				

Mã Tham chiếu	Mã Kiến thức	Kiến thức	Mã Kỹ năng	Kỹ năng	4	3	2	1
	KT163	Kiến thức về các tiêu chuẩn an toàn dữ liệu thẻ thanh toán (PCI).	KN118	Kỹ năng quản lý mối quan hệ với khách hàng, bao gồm xác định nhu cầu / yêu cầu của khách hàng, quản lý kỳ vọng của khách hàng và thể hiện cam kết cung cấp chất lượng sản phẩm.				
	KT164	Kiến thức về các tiêu chuẩn an toàn dữ liệu thông tin y tế, sức khỏe cá nhân.	KN119	Kỹ năng thực hiện phân tích hệ thống mục tiêu.				
	KT169	Kiến thức về luật pháp, chính sách, thủ tục hoặc quản trị an toàn thông tin mạng cho các hạ tầng quan trọng.	KN120	Kỹ năng chuẩn bị và trình bày các cuộc họp giao ban.				
	KT182	Kiến thức về chương trình phân loại thông tin và các quy trình đối với xâm phạm thông tin.	KN121	Kỹ năng chuẩn bị kế hoạch và các thư từ liên quan.				
	KT198	Kiến thức về hệ thống nhúng.	KN122	Kỹ năng ưu tiên ngôn ngữ mục tiêu quan trọng.				
	KT208	Kiến thức về các nguyên tắc, công cụ và kỹ thuật kiểm thử xâm nhập.	KN123	Kỹ năng xử lý dữ liệu thu thập được để phân tích tiếp.				
	KT247	Kiến thức về các biện pháp kiểm soát liên quan đến việc sử dụng, xử lý, lưu trữ và truyền dữ liệu.	KN124	Kỹ năng phân tích để hỗ trợ viết báo cáo hành động theo từng giai đoạn.				
	KT248	Kiến thức về rủi ro bảo mật ứng dụng (ví dụ: Danh sách top 10 lỗ hổng owasp).	KN126	Kỹ năng nhận xét và chỉnh sửa sản phẩm đánh giá.				
			KN127	Kỹ năng xem xét và chỉnh sửa kế hoạch.				
			KN128	Kỹ năng điều chỉnh phân tích theo các cấp độ cần thiết (ví dụ: phân loại và tổ chức).				
			KN129	Kỹ năng phát triển mục tiêu hỗ trợ trực tiếp cho nghiệp vụ thu thập.				

Mã Tham chiếu	Mã Kiến thức	Kiến thức	Mã Kỹ năng	Kỹ năng	4	3	2	1
			KN130	Kỹ năng xác định sự bất thường của mạng mục tiêu (ví dụ: xâm nhập, luồng dữ liệu hoặc xử lý, triển khai các công nghệ mới).				
			KN131	Kỹ năng về kỹ thuật viết báo cáo.				
			KN135	Kỹ năng sử dụng phản hồi để cải thiện quy trình, sản phẩm và dịch vụ.				
			KN138	Kỹ năng tiếp cận thông tin về tài sản hiện có, cách sử dụng.				
			KN139	Kỹ năng truy cập cơ sở dữ liệu về các chương trình/kế hoạch/chỉ thị/hướng dẫn.				
			KN140	Kỹ năng phân tích hướng dẫn chiến lược cho các vấn đề cần làm rõ và/hoặc hướng dẫn bổ sung.				
			KN141	Kỹ năng phân tích mục tiêu hoặc mối đe dọa.				
			KN142	Kỹ năng xây dựng kế hoạch thu thập thông tin thể hiện rõ nguyên tắc để thu thập thông tin cần thiết.				
			KN143	Kỹ năng đánh giá các yêu cầu cung cấp thông tin để xác định xem thông tin phản hồi có tồn tại hay không.				
			KN144	Kỹ năng trích xuất thông tin từ các công cụ và ứng dụng có sẵn liên quan đến yêu cầu thu thập và quản lý hoạt động thu thập.				
			KN147	Kỹ năng áp dụng các nguyên tắc an toàn thông tin mạng và quyền riêng tư đối với các yêu cầu của tổ chức (liên quan đến tính bí mật, tính toàn vẹn, tính khả dụng, xác thực, chống chối bỏ).				

Mã Tham chiếu	Mã Kiến thức	Kiến thức	Mã Kỹ năng	Kỹ năng	4	3	2	1
			KN148	Kỹ năng sử dụng sơ đồ và quy trình báo cáo của nhà cung cấp dịch vụ an toàn toàn thông tin mạng.				
			KN149	Kỹ năng xác định các vấn đề về an toàn thông tin mạng và quyền riêng tư xuất phát từ các mỗi quan hệ bên trong, khách hàng bên ngoài và các tổ chức đối tác.				
CSSS 2	**Ứng cứu sự cố**				**x**	**x**	**x**	**x**
	KT001	Kiến thức về các khái niệm và giao thức mạng máy tính và phương pháp luận về an toàn thông tin mạng.	KN002	Kỹ năng xác định, nắm bắt, lưu trữ và báo cáo phần mềm độc hại.				
	KT002	Kiến thức về các quy trình quản lý rủi ro (ví dụ: các phương pháp đánh giá và giảm thiểu rủi ro).	KN020	Kỹ năng bảo quản tính toàn vẹn của bằng chứng theo quy trình thao tác tiêu chuẩn hoặc tiêu chuẩn quốc gia.				
	KT003	Kiến thức về luật, quy định, chính sách và đạo đức nghề nghiệp liên quan đến an toàn thông tin mạng và quyền riêng tư.	KN042	Kỹ năng bảo đảm an toàn mạng thông tin liên lạc.				
	KT004	Kiến thức về an toàn thông tin mạng và các nguyên tắc quyền riêng tư.	KN043	Kỹ năng nhận biết, phân loại các loại điểm yếu và các hình thức tấn công liên quan.				
	KT005	Kiến thức về các mối đe dọa và điểm yếu an toàn thông tin mạng.	KN044	Kỹ năng bảo vệ mạng khỏi phần mềm độc hại. (Ví dụ: NIPS, chống phần mềm độc hại, hạn chế/ngăn chặn thiết bị bên ngoài, bộ lọc thư rác).				
	KT006	Kiến thức về các ảnh hưởng đối với hoạt động do mất an toàn thông tin mạng.	KN045	Kỹ năng thực hiện đánh giá thiệt hại.				
	KT019	Kiến thức về sao lưu và phục hồi dữ liệu.	KN092	Kỹ năng sử dụng các công cụ hiệu chỉnh tương quan sự kiện an toàn thông tin.				

Mã Tham chiếu	Mã Kiến thức	Kiến thức	Mã Kỹ năng	Kỹ năng	4	3	2	1
	KT021	Kiến thức về kế hoạch duy trì hoạt động và khôi phục thảm họa.	KN146	Kỹ năng thiết kế ứng phó sự cố cho các mô hình dịch vụ đám mây.				
	KT027	Kiến thức về cơ chế kiểm soát truy cập máy chủ/mạng (ví dụ: danh sách kiểm soát truy cập, danh sách khả năng).						
	KT028	Kiến thức về các dịch vụ mạng và giao thức kết nối mạng.						
	KT035	Kiến thức về các loại sự cố, ứng phó sự cố và tiến trình phản hồi sự cố an toàn thông tin mạng.						
	KT036	Kiến thức về phương pháp ứng phó và xử lý sự cố an toàn thông tin mạng.						
	KT040	Kiến thức về các phương pháp và kỹ thuật phát hiện xâm nhập để phát hiện việc xâm nhập máy chủ và mạng.						
	KT050	Kiến thức về các phương pháp phân tích lưu lượng mạng.						
	KT054	Kiến thức về phân tích mức gói tin (packet-level).						
	KT060	Kiến thức về các mối đe dọa và điểm yếu của hệ thống và ứng dụng (ví dụ: tràn bộ đệm (buffer overflow), mã di động (mobile code), cross-site scripting, PL/SQL injection, mã độc,...).						
	KT084	Kiến thức về các thành phần một cuộc tấn công mạng và mối quan hệ của một cuộc tấn công mạng đối với các mối đe dọa và điểm yếu.						

Mã Tham chiếu	Mã Kiến thức	Kiến thức	Mã Kỹ năng	Kỹ năng	4	3	2	1
	KT113	Kiến thức về các chính sách, thủ tục và quy định về bảo vệ mạng và an toàn thông tin.						
	KT115	Kiến thức về các loại tấn công khác nhau (ví dụ: thụ động, chủ động, nội gián, cận cảnh, phân tán tấn công).						
	KT116	Kiến thức về các đối tượng tấn công mạng (ví dụ: nghiệp dư (script kiddies), nội gián, tài trợ quốc gia,...).						
	KT117	Kiến thức về kỹ thuật quản trị hệ thống, mạng và cứng hóa (hardening) hệ điều hành.						
	KT126	Kiến thức về các giai đoạn tấn công mạng (ví dụ: trinh sát, dò quét, liệt kê, truy nhập hệ thống, leo thang đặc quyền, duy trì truy cập, khai thác mạng, xóa dấu vết).						
	KT127	Kiến thức về các khái niệm kiến trúc an toàn thông tin mạng bao gồm cấu trúc liên kết (topology), giao thức, các thành phần và nguyên tắc (ví dụ: phòng thủ chiều sâu defense-in-depth).						
	KT152	Kiến thức về mô hình OSI và các giao thức mạng cơ bản (ví dụ: TCP/IP).						
	KT156	Kiến thức về các mô hình dịch vụ đám mây và cách các mô hình đó có thể hạn chế ứng cứu sự cố.						
	KT161	Kiến thức về các khái niệm và phương pháp phân tích mã độc.						

Mã Tham chiếu	Mã Kiến thức	Kiến thức	Mã Kỹ năng	Kỹ năng	4	3	2	1
	KT182	Kiến thức về chương trình phân loại thông tin và các quy trình đối với xâm phạm thông tin.						
	KT203	Kiến thức về các giao thức mạng như TCP/IP, DHCP, DNS và các dịch vụ thư mục.						
	KT241	Kiến thức về các giao thức mạng và định tuyến phổ biến (ví dụ: TCP/IP), các dịch vụ (ví dụ: web, thư, DNS) và cách chúng tương tác để cung cấp kết nối mạng.						
	KT248	Kiến thức về rủi ro bảo mật ứng dụng (ví dụ: Danh sách top 10 lỗ hổng owasp).						
CSSS 3	**Kiểm tra, đánh giá điểm yếu**				**x**	**x**	**x**	**x**
	KT001	Kiến thức về các khái niệm và giao thức mạng máy tính và phương pháp luận về an toàn thông tin mạng.	KN001	Kỹ năng tiến hành rà quét điểm yếu và nhận biết các điểm yếu để đảm bảo an toàn các hệ thống.				
	KT002	Kiến thức về các quy trình quản lý rủi ro (ví dụ: các phương pháp đánh giá và giảm thiểu rủi ro).	KN006	Kỹ năng đánh giá mức độ an toàn thông tin của hệ thống và mô hình thiết kế.				
	KT003	Kiến thức về luật, quy định, chính sách và đạo đức nghề nghiệp liên quan đến an toàn thông tin mạng và quyền riêng tư.	KN012	Kỹ năng sử dụng các công cụ phát hiện xâm nhập trên máy chủ và mạng. (ví dụ: Snort).				
	KT004	Kiến thức về an toàn thông tin mạng và các nguyên tắc quyền riêng tư.	KN019	Kỹ năng bắt chước các hành vi đe dọa.				
	KT005	Kiến thức về các mối đe dọa và điểm yếu an toàn thông tin mạng.	KN022	Kỹ năng sử dụng các công cụ và kỹ thuật kiểm thử xâm nhập.				
	KT006	Kiến thức về các ảnh hưởng đối với hoạt động do mất an toàn thông tin mạng.	KN023	Kỹ năng sử dụng các kỹ thuật tấn công phi kỹ thuật (ví dụ: phishing, baiting, tailgating, v.v.).				

Mã Tham chiếu	Mã Kiến thức	Kiến thức	Mã Kỹ năng	Kỹ năng	4	3	2	1
	KT009	Kiến thức về các điểm yếu ứng dụng.	KN046	Kỹ năng sử dụng các công cụ phân tích mạng để xác định các điểm yếu. (ví dụ: fuzzing, nmap, v.v.).				
	KT018	Kiến thức về mật mã và các khái niệm quản lý khóa mật mã.	KN064	Kỹ năng xem lại nhật ký để xác định bằng chứng về những lần xâm nhập trong quá khứ.				
	KT019	Kiến thức về sao lưu và phục hồi dữ liệu.	KN075	Kỹ năng thực hiện đánh giá điểm yếu an toàn ứng dụng.				
	KT027	Kiến thức về cơ chế kiểm soát truy cập máy chủ/mạng (ví dụ: danh sách kiểm soát truy cập, danh sách khả năng).	KN090	Kỹ năng thực hiện đánh giá tác động/rủi ro.				
	KT038	Kiến thức về các nguyên tắc và yêu cầu an toàn thông tin mạng và riêng tư (liên quan đến tính bí mật, tính toàn vẹn, tính khả dụng, xác thực, chống chối bỏ).	KN145	Kỹ năng để phát triển những hiểu biết chuyên sâu về bối cảnh môi trường đe dọa của tổ chức				
	KT048	Kiến thức về truy cập mạng, danh tính và quản lý truy cập (ví dụ: hạ tầng khóa công khai, Oauth, OpenID, SAML, SPML).	KN147	Kỹ năng áp dụng các nguyên tắc an toàn thông tin mạng và quyền riêng tư đối với các yêu cầu của tổ chức (liên quan đến tính bí mật, tính toàn vẹn, tính khả dụng, xác thực, chống chối bỏ).				
	KT053	Kiến thức về cách lưu lượng truyền qua mạng (ví dụ: Giao thức TCP, IP, Mô hình OSI,...).						
	KT059	Kiến thức về cấu trúc ngôn ngữ lập trình và logic.						
	KT060	Kiến thức về các mối đe dọa và điểm yếu của hệ thống và ứng dụng (ví dụ: tràn bộ đệm (buffer overflow), mã di động (mobile code), cross-site scripting, PL/SQL injection, mã độc,...).						

Mã Tham chiếu	Mã Kiến thức	Kiến thức	Mã Kỹ năng	Kỹ năng	4	3	2	1
	KT074	Kiến thức về các công cụ đánh giá hệ thống và kỹ thuật xác định lỗi.						
	KT084	Kiến thức về các thành phần một cuộc tấn công mạng và mối quan hệ của một cuộc tấn công mạng đối với các mối đe dọa và điểm yếu.						
	KT106	Kiến thức về ngôn ngữ máy tính thông dịch và biên dịch.						
	KT115	Kiến thức về các loại tấn công khác nhau (ví dụ: thụ động, chủ động, nội gián, cận cảnh, phân tán tấn công).						
	KT116	Kiến thức về các đối tượng tấn công mạng (ví dụ: nghiệp dư (script kiddies), nội gián, tài trợ quốc gia,...).						
	KT117	Kiến thức về kỹ thuật quản trị hệ thống, mạng và cứng hóa (hardening) hệ điều hành.						
	KT126	Kiến thức về các giai đoạn tấn công mạng (ví dụ: trinh sát, dò quét, liệt kê, truy nhập hệ thống, leo thang đặc quyền, duy trì truy cập, khai thác mạng, xóa dấu vết).						
	KT127	Kiến thức về các khái niệm kiến trúc an toàn thông tin mạng bao gồm cấu trúc liên kết (topology), giao thức, các thành phần và nguyên tắc (ví dụ: phòng thủ chiều sâu defense-in-depth).						
	KT144	Kiến thức về các mô hình bảo mật (ví dụ: mô hình Bell-LaPadula, mô hình Biba, Mô hình Clark Wilson).						

Mã Tham chiếu	Mã Kiến thức	Kiến thức	Mã Kỹ năng	Kỹ năng	4	3	2	1
	KT146	Kiến thức về nguyên tắc đạo đức và kỹ thuật hack.						
	KT148	Kiến thức về các khái niệm sao lưu và phục hồi dữ liệu.						
	KT154	Kiến thức về các khái niệm quản trị hệ thống cho hệ điều hành, chẳng hạn như nhưng không giới hạn cho các hệ điều hành Unix/Linux, IOS, Android và Windows.						
	KT167	Kiến thức về hạ tầng hỗ trợ để đảm bảo an toàn, hiệu suất và độ tin cậy.						
	KT182	Kiến thức về chương trình phân loại thông tin và các quy trình đối với xâm phạm thông tin.						
	KT189	Kiến thức về phân tích gói tin bằng các công cụ thích hợp (ví dụ: Wireshark, tcpdump).						
	KT192	Kiến thức về mật mã học.						
	KT203	Kiến thức về các giao thức mạng như TCP/IP, DHCP, DNS và các dịch vụ thư mục.						
	KT208	Kiến thức về các nguyên tắc, công cụ và kỹ thuật kiểm thử xâm nhập.						
	KT209	Kiến thức về các mối đe dọa trong môi trường của tổ chức.						
	KT248	Kiến thức về rủi ro bảo mật ứng dụng (ví dụ: Danh sách top 10 lỗ hổng owasp).						

Mã Tham chiếu	Mã Kiến thức	Kiến thức	Mã Kỹ năng	Kỹ năng	4	3	2	1
CSSS 4	**Giám sát an toàn thông tin**				**x**	**x**	**x**	**x**
	KT001	Kiến thức về các khái niệm và giao thức mạng máy tính và phương pháp luận về an toàn thông tin mạng.	KN008	Kỹ năng phát triển và triển khai chữ ký số.				
	KT002	Kiến thức về các quy trình quản lý rủi ro (ví dụ: các phương pháp đánh giá và giảm thiểu rủi ro).	KN012	Kỹ năng sử dụng các công cụ phát hiện xâm nhập trên máy chủ và mạng. (ví dụ: Snort).				
	KT003	Kiến thức về luật, quy định, chính sách và đạo đức nghề nghiệp liên quan đến an toàn thông tin mạng và quyền riêng tư.	KN013	Kỹ năng xác định cách thức hoạt động của hệ thống bảo mật (bao gồm khả năng phục hồi và khả năng tin cậy) và những thay đổi về điều kiện, hoạt động hoặc môi trường sẽ ảnh hưởng như thế nào đến những kết quả này.				
	KT004	Kiến thức về an toàn thông tin mạng và các nguyên tắc quyền riêng tư.	KN017	Kỹ năng đánh giá tính đầy đủ của an toàn thiết kế.				
	KT005	Kiến thức về các mối đe dọa và điểm yếu an toàn thông tin mạng.	KN025	Kỹ năng sử dụng các phương pháp xử lý sự cố.				
	KT006	Kiến thức về các ảnh hưởng đối với hoạt động do mất an toàn thông tin mạng.	KN026	Kỹ năng sử dụng bộ phân tích giao thức.				
	KT007	Kiến thức về phương pháp xác thực, ủy quyền và kiểm soát truy cập.	KN031	Kỹ năng thu thập nguồn dữ liệu về phòng thủ mạng.				
	KT013	Kiến thức về các công cụ bảo vệ và đánh giá điểm yếu an toàn thông tin mạng và khả năng của các công cụ.	KN043	Kỹ năng nhận biết, phân loại các loại điểm yếu và các hình thức tấn công liên quan.				
	KT015	Kiến thức về thuật toán máy tính.	KN056	Kỹ năng đọc và phiên dịch các dấu hiệu nhận biết (signatures) (ví dụ: snort).				

Mã Tham chiếu	Mã Kiến thức	Kiến thức	Mã Kỹ năng	Kỹ năng	4	3	2	1
	KT017	Kiến thức về các thuật toán mã hóa	KN081	Kỹ năng đánh giá các biện pháp kiểm soát an toàn dựa trên các nguyên tắc và nguyên lý an toàn thông tin mạng.				
	KT018	Kiến thức về mật mã và các khái niệm quản lý khóa mật mã	KN084	Kỹ năng thực hiện phân tích mức gói tin.				
	KT020	Kiến thức về hệ thống cơ sở dữ liệu.	KN086	Kỹ năng nhận điểm yếu về an toàn các hệ thống. (ví dụ: rà quét điểm yếu và xem xét sự tuân thủ).				
	KT027	Kiến thức về cơ chế kiểm soát truy cập máy chủ/mạng (ví dụ: danh sách kiểm soát truy cập, danh sách khả năng).	KN088	Kỹ năng thực hiện phân tích xu hướng (trend).				
	KT034	Kiến thức về các nguồn phổ biến thông tin về điểm yếu bảo mật (ví dụ: cảnh báo, tư vấn và bản tin,...).	KN147	Kỹ năng áp dụng các nguyên tắc an toàn thông tin mạng và quyền riêng tư đối với các yêu cầu của tổ chức (liên quan đến tính bí mật, tính toàn vẹn, tính khả dụng, xác thực, chống chối bỏ).				
	KT036	Kiến thức về phương pháp ứng phó và xử lý sự cố an toàn thông tin mạng.	KN148	Kỹ năng sử dụng sơ đồ và quy trình báo cáo của nhà cung cấp dịch vụ an toàn toàn thông tin mạng.				
	KT038	Kiến thức về các nguyên tắc và yêu cầu an toàn thông tin mạng và riêng tư (liên quan đến tính bí mật, tính toàn vẹn, tính khả dụng, xác thực, chống chối bỏ).						
	KT040	Kiến thức về các phương pháp và kỹ thuật phát hiện xâm nhập để phát hiện việc xâm nhập máy chủ và mạng.						
	KT042	Kiến thức về các nguyên tắc và phương pháp an toàn thông tin (ví dụ: tường lửa, DMZ, mã hóa).						

Mã Tham chiếu	Mã Kiến thức	Kiến thức	Mã Kỹ năng	Kỹ năng	4	3	2	1
	KT048	Kiến thức về truy cập mạng, danh tính và quản lý truy cập (ví dụ: hạ tầng khóa công khai, Oauth, OpenID, SAML, SPML).						
	KT050	Kiến thức về các phương pháp phân tích lưu lượng mạng.						
	KT051	Kiến thức về các công nghệ mới và mới nổi lĩnh vực công nghệ thông tin và an toàn thông tin mạng.						
	KT052	Kiến thức về hệ điều hành.						
	KT053	Kiến thức về cách lưu lượng truyền qua mạng (ví dụ: Giao thức TCP, IP, Mô hình OSI,...).						
	KT056	Kiến thức về các biện pháp kiểm soát truy cập dựa trên chính sách và thích ứng với rủi ro.						
	KT060	Kiến thức về các mối đe dọa và điểm yếu của hệ thống và ứng dụng (ví dụ: tràn bộ đệm (buffer overflow), mã di động (mobile code), cross-site scripting, PL/SQL injection, mã độc,...).						
	KT063	Kiến thức về các khái niệm chính trong quản lý bảo mật an toàn thông tin mạng (ví dụ: Quản lý phát hành, Quản lý bản vá).						
	KT064	Kiến thức về các công cụ, phương pháp và kỹ thuật thiết kế hệ thống bảo mật.						
	KT078	Kiến thức về các khái niệm viễn thông (ví dụ: Kênh truyền, đa kênh,…).						

Mã Tham chiếu	Mã Kiến thức	Kiến thức	Mã Kỹ năng	Kỹ năng	4	3	2	1
	KT079	Kiến thức về cấu trúc và quy trình báo cáo của nhà cung cấp dịch vụ an toàn thông tin mạng.						
	KT083	Kiến thức về bảo mật Mạng riêng ảo (VPN).						
	KT084	Kiến thức về các thành phần một cuộc tấn công mạng và mối quan hệ của một cuộc tấn công mạng đối với các mối đe dọa và điểm yếu.						
	KT085	Kiến thức về rà soát nguy cơ nội bộ, báo cáo, các công cụ rà soát, các luật/quy định.						
	KT088	Kiến thức về chiến thuật, kỹ thuật và quy trình đối thủ.						
	KT089	Kiến thức về các công cụ mạng (ví dụ: ping, traceroute, nslookup).						
	KT090	Kiến thức các nguyên tắc phòng thủ chiều sâu (defense-in-depth) và kiến trúc an toàn mạng.						
	KT091	Kiến thức về các loại kết nối mạng khác nhau (ví dụ: LAN, WAN, MAN, WLAN, WWAN).						
	KT092	Kiến thức về các phần mở rộng tên tệp (ví dụ: .dll, .bat, .zip, .pcap, .gzip).						
	KT106	Kiến thức về ngôn ngữ máy tính thông dịch và biên dịch.						
	KT107	Kiến thức về các quy trình, khả năng và hạn chế của quản lý thu thập.						
	KT108	Kiến thức về thu thập hệ thống front-end, bao gồm thu thập, lọc lưu lượng và lựa chọn.						

Mã Tham chiếu	Mã Kiến thức	Kiến thức	Mã Kỹ năng	Kỹ năng	4	3	2	1
	KT113	Kiến thức về các chính sách, thủ tục và quy định về bảo vệ mạng và an toàn thông tin.						
	KT114	Kiến thức về các vectơ tấn công phổ biến trên lớp mạng.						
	KT115	Kiến thức về các loại tấn công khác nhau (ví dụ: thụ động, chủ động, nội gián, cận cảnh, phân tán tấn công).						
	KT116	Kiến thức về các đối tượng tấn công mạng (ví dụ: nghiệp dư (script kiddies), nội gián, tài trợ quốc gia,...).						
	KT117	Kiến thức về kỹ thuật quản trị hệ thống, mạng và cứng hóa (hardening) hệ điều hành.						
	KT118	Kiến thức về luật, nghị định, chỉ thị, quy định hiện hành về an toàn thông tin.						
	KT126	Kiến thức về các giai đoạn tấn công mạng (ví dụ: trinh sát, dò quét, liệt kê, truy nhập hệ thống, leo thang đặc quyền, duy trì truy cập, khai thác mạng, xóa dấu vết).						
	KT127	Kiến thức về các khái niệm kiến trúc an toàn thông tin mạng bao gồm cấu trúc liên kết (topology), giao thức, các thành phần và nguyên tắc (ví dụ: phòng thủ chiều sâu defense-in-depth).						
	KT128	Kiến thức về các nguyên tắc, mô hình, phương pháp quản lý hệ thống mạng và các công cụ.						
	KT137	Kiến thức về các phương pháp mã hóa.						

Mã Tham chiếu	Mã Kiến thức	Kiến thức	Mã Kỹ năng	Kỹ năng	4	3	2	1
	KT138	Kiến thức tác động của nhận biết vi rút, mã độc và các cuộc tấn công.						
	KT139	Kiến thức về các cổng và dịch vụ Windows / Unix.						
	KT144	Kiến thức về các mô hình bảo mật (ví dụ: mô hình Bell-LaPadula, mô hình Biba, Mô hình Clark Wilson).						
	KT152	Kiến thức về mô hình OSI và các giao thức mạng cơ bản (ví dụ: TCP/IP).						
	KT153	Kiến thức về luật, cơ quan pháp lý, các hạn chế và quy định liên quan đến hoạt động phòng thủ trên không gian mạng.						
	KT162	Kiến thức về các tiêu chuẩn an toàn thông tin cá nhân, dữ liệu cá nhân.						
	KT163	Kiến thức về các tiêu chuẩn an toàn dữ liệu thẻ thanh toán (PCI).						
	KT164	Kiến thức về các tiêu chuẩn an toàn dữ liệu thông tin y tế, sức khỏe cá nhân.						
	KT184	Kiến thức về các phương pháp kiểm tra và đánh giá bảo mật hệ thống.						
	KT188	Kiến thức về thiết kế biện pháp đối phó với các rủi ro bảo mật đã xác định.						
	KT190	Kiến thức về việc sử dụng các công cụ chia mạng (sub-netting tools).						

Mã Tham chiếu	Mã Kiến thức	Kiến thức	Mã Kỹ năng	Kỹ năng	4	3	2	1
	KT195	Kiến thức về các công cụ dòng lệnh của hệ điều hành.						
	KT198	Kiến thức về hệ thống nhúng.						
	KT200	Kiến thức về các công cụ và ứng dụng Hệ thống phát hiện xâm nhập (IDS)/Hệ thống ngăn ngừa xâm nhập (IPS).						
	KT203	Kiến thức về các giao thức mạng như TCP/IP, DHCP, DNS và các dịch vụ thư mục.						
	KT207	Kiến thức về cách sử dụng các công cụ phân tích mạng để xác định các điểm yếu.						
	KT208	Kiến thức về các nguyên tắc, công cụ và kỹ thuật kiểm thử xâm nhập.						
	KT248	Kiến thức về rủi ro bảo mật ứng dụng (ví dụ: Danh sách top 10 lỗ hổng owasp).						
CSSS 5	**An toàn hạ tầng thông tin**				**x**	**x**	**x**	**x**
	KT001	Kiến thức về các khái niệm và giao thức mạng máy tính và phương pháp luận về an toàn thông tin mạng.	KN005	Kỹ năng áp dụng các kiểm soát truy cập máy chủ/mạng (ví dụ: danh sách kiểm soát truy cập).				
	KT002	Kiến thức về các quy trình quản lý rủi ro (ví dụ: các phương pháp đánh giá và giảm thiểu rủi ro).	KN024	Kỹ năng điều chỉnh cảm biến (sensor).				
	KT003	Kiến thức về luật, quy định, chính sách và đạo đức nghề nghiệp liên quan đến an toàn thông tin mạng và quyền riêng tư.	KN025	Kỹ năng sử dụng các phương pháp xử lý sự cố.				

Mã Tham chiếu	Mã Kiến thức	Kiến thức	Mã Kỹ năng	Kỹ năng	4	3	2	1
	KT004	Kiến thức về an toàn thông tin mạng và các nguyên tắc quyền riêng tư.	KN027	Kỹ năng sử dụng thiết bị Mạng riêng ảo (VPN) và mã hóa.				
	KT005	Kiến thức về các mối đe dọa và điểm yếu an toàn thông tin mạng.	KN042	Kỹ năng bảo đảm an toàn mạng thông tin liên lạc.				
	KT006	Kiến thức về các ảnh hưởng đối với hoạt động do mất an toàn thông tin mạng.	KN044	Kỹ năng bảo vệ mạng khỏi phần mềm độc hại. (Ví dụ: NIPS, chống phần mềm độc hại, hạn chế/ngăn chặn thiết bị bên ngoài, bộ lọc thư rác).				
	KT019	Kiến thức về sao lưu và phục hồi dữ liệu.	KN065	Kỹ năng về các kỹ thuật cứng hóa (hardening) hệ thống, mạng và hệ điều hành. (ví dụ: xóa các dịch vụ không cần thiết, chính sách mật khẩu, phân đoạn mạng, bật ghi nhật ký, ít đặc quyền nhất, v.v.).				
	KT027	Kiến thức về cơ chế kiểm soát truy cập máy chủ/mạng (ví dụ: danh sách kiểm soát truy cập, danh sách khả năng).	KN067	Kỹ năng xử lý sự cố và chẩn đoán các bất thường về cơ sở hạ tầng phòng thủ không gian mạng và giải quyết vấn đề.				
	KT036	Kiến thức về phương pháp ứng phó và xử lý sự cố an toàn thông tin mạng.	KN147	Kỹ năng áp dụng các nguyên tắc an toàn thông tin mạng và quyền riêng tư đối với các yêu cầu của tổ chức (liên quan đến tính bí mật, tính toàn vẹn, tính khả dụng, xác thực, chống chối bỏ).				
	KT038	Kiến thức về các nguyên tắc và yêu cầu an toàn thông tin mạng và riêng tư (liên quan đến tính bí mật, tính toàn vẹn, tính khả dụng, xác thực, chống chối bỏ).						
	KT050	Kiến thức về các phương pháp phân tích lưu lượng mạng.						

Mã Tham chiếu	Mã Kiến thức	Kiến thức	Mã Kỹ năng	Kỹ năng	4	3	2	1
	KT053	Kiến thức về cách lưu lượng truyền qua mạng (ví dụ: Giao thức TCP, IP, Mô hình OSI,...).						
	KT054	Kiến thức về phân tích mức gói tin (packet-level).						
	KT083	Kiến thức về bảo mật Mạng riêng ảo (VPN).						
	KT084	Kiến thức về các thành phần một cuộc tấn công mạng và mối quan hệ của một cuộc tấn công mạng đối với các mối đe dọa và điểm yếu.						
	KT105	Kiến thức về các công nghệ lọc web.						
	KT113	Kiến thức về các chính sách, thủ tục và quy định về bảo vệ mạng và an toàn thông tin.						
	KT127	Kiến thức về các khái niệm kiến trúc an toàn thông tin mạng bao gồm cấu trúc liên kết (topology), giao thức, các thành phần và nguyên tắc (ví dụ: phòng thủ chiều sâu defense-in-depth).						
	KT145	Kiến thức cơ bản về hệ thống, mạng và kỹ thuật cứng hóa hệ điều hành.						
	KT160	Kiến thức về các thủ tục, nguyên tắc và phương pháp kiểm tra.						
	KT174	Kiến thức về các bản ghi truyền tải (ví dụ: Bluetooth, RFID, IR,Wi-Fi…)						
	KT200	Kiến thức về các công cụ và ứng dụng Hệ thống phát hiện xâm nhập (IDS)/Hệ thống ngăn ngừa xâm nhập (IPS).						

Mã Tham chiếu	Mã Kiến thức	Kiến thức	Mã Kỹ năng	Kỹ năng	4	3	2	1
	KT203	Kiến thức về các giao thức mạng như TCP/IP, DHCP, DNS và các dịch vụ thư mục.						
	KT205	Kiến thức về phân tích lưu lượng mạng (các công cụ, phương pháp luận, quy trình).						
CSSS 6	**Điều tra số**					**x**	**x**	**x**
	KT001	Kiến thức về các khái niệm và giao thức mạng máy tính và phương pháp luận về an toàn thông tin mạng.	KN015	Kỹ năng trong việc phát triển, kiểm tra và thực hiện các kế hoạch dự phòng, khôi phục hạ tầng mạng.				
	KT002	Kiến thức về các quy trình quản lý rủi ro (ví dụ: các phương pháp đánh giá và giảm thiểu rủi ro).	KN020	Kỹ năng bảo quản tính toàn vẹn của bằng chứng theo quy trình thao tác tiêu chuẩn hoặc tiêu chuẩn quốc gia.				
	KT003	Kiến thức về luật, quy định, chính sách và đạo đức nghề nghiệp liên quan đến an toàn thông tin mạng và quyền riêng tư.	KN030	Kỹ năng phân tích kết xuất bộ nhớ để trích xuất thông tin.				
	KT004	Kiến thức về an toàn thông tin mạng và các nguyên tắc quyền riêng tư.	KN032	Kỹ năng xác định và trích xuất dữ liệu quan trọng của điều tra số trong các phương tiện đa dạng.				
	KT005	Kiến thức về các mối đe dọa và điểm yếu an toàn thông tin mạng.	KN033	Kỹ năng xác định, sửa đổi và thao tác các ứng dụng thành phần hệ thống trong Windows, Unix hoặc Linux (ví dụ: mật khẩu, tài khoản người dùng, tệp).				
	KT006	Kiến thức về các ảnh hưởng đối với hoạt động do mất an toàn thông tin mạng.	KN034	Kỹ năng thu thập, xử lý, đóng gói, vận chuyển và lưu trữ bằng chứng điện tử để tránh thay đổi, mất mát, hư hỏng vật lý hoặc phá hủy dữ liệu.				
	KT017	Kiến thức về các thuật toán mã hóa.	KN035	Kỹ năng thiết lập máy trạm điều tra số chuyên dụng.				

Mã Tham chiếu	Mã Kiến thức	Kiến thức	Mã Kỹ năng	Kỹ năng	4	3	2	1
	KT019	Kiến thức về sao lưu và phục hồi dữ liệu.	KN036	Kỹ năng sử dụng các bộ công cụ điều tra số (ví dụ: EnCase, Sleuthkit, FTK).				
	KT036	Kiến thức về phương pháp ứng phó và xử lý sự cố an toàn thông tin mạng.	KN038	Kỹ năng sử dụng máy ảo. (Ví dụ: Microsoft Hyper-V, VMWare, VirtualBox, v.v.).				
	KT052	Kiến thức về hệ điều hành.	KN039	Kỹ năng tháo lắp vật lý các máy tính cá nhân.				
	KT060	Kiến thức về các mối đe dọa và điểm yếu của hệ thống và ứng dụng (ví dụ: tràn bộ đệm (buffer overflow), mã di động (mobile code), cross-site scripting, PL/SQL injection, mã độc,...).	KN040	Kỹ năng thực hiện phân tích điều tra trong nhiều môi trường hệ điều hành (ví dụ: hệ thống thiết bị di động).				
	KT065	Kiến thức về hệ điều hành máy chủ và máy khách/trạm.	KN049	Kỹ năng phân tích chuyên sâu về thu thập mã độc hại (ví dụ: điều tra số về phần mềm mã độc)				
	KT066	Kiến thức về các công cụ đánh giá máy chủ và kỹ thuật xác định lỗi.	KN050	Kỹ năng sử dụng các công cụ phân tích nhị phân (ví dụ: Hexedit, mã lệnh xxd, hexdump).				
	KT087	Kiến thức về các thành phần và kiến trúc máy tính vật lý, bao gồm các chức năng của các thành phần và thiết bị ngoại vi khác nhau (ví dụ: CPU, NIC, lưu trữ dữ liệu).	KN051	Kỹ năng trong các hàm băm một chiều (ví dụ: Thuật toán băm SHA, MD5).				
	KT093	Kiến thức về các hệ thống tập tin thực thi (ví dụ: NTFS, FAT, EXT).	KN052	Kỹ năng phân tích các loại mã bất thường là độc hại hay lành tính				
	KT094	Kiến thức về các quy trình thu giữ và bảo quản bằng chứng số.	KN053	Kỹ năng phân tích dữ liệu biến động.				
	KT095	Kiến thức về các phương pháp hack.	KN054	Kỹ năng xác định các kỹ thuật xáo trộn (obfuscation)				
	KT096	Kiến thức về các tác động điều tra với phần cứng, Hệ điều hành và các công nghệ mạng.	KN055	Kỹ năng phiên dịch kết quả của trình gỡ lỗi để xác định chiến thuật, kỹ thuật và quy trình.				

Mã Tham chiếu	Mã Kiến thức	Kiến thức	Mã Kỹ năng	Kỹ năng	4	3	2	1
	KT097	Kiến thức về quản trị pháp lý liên quan đến khả năng chấp nhận (ví dụ: Quy tắc về bằng chứng).	KN069	Kỹ năng phân tích mã độc.				
	KT098	Kiến thức về các quy trình thu thập, đóng gói, vận chuyển và lưu trữ bằng chứng số trong khi duy trì chuỗi quy trình.	KN070	Kỹ năng tiến hành phân tích mức bit.				
	KT100	Kiến thức về loại và thu thập dữ liệu ổn định (persistent data).	KN071	Kỹ năng xử lý bằng chứng số, bao gồm việc bảo vệ và tạo bản sao hợp pháp của bằng chứng.				
	KT101	Kiến thức về thu thập, kỹ thuật tìm kiếm / phân tích, công cụ và cookie của thư điện tử.	KN084	Kỹ năng thực hiện phân tích mức gói tin.				
	KT102	Kiến thức về tệp tin hệ thống (ví dụ: tệp nhật ký, tệp đăng ký, tệp cấu hình) chứa thông tin liên quan và nơi tìm các tệp hệ thống đó.						
	KT103	Kiến thức về các loại dữ liệu điều tra số và cách nhận biết.						
	KT104	Kiến thức về khả năng triển khai điều tra số.						
	KT109	Kiến thức về các công cụ tương quan sự kiện an toàn thông tin mạng.						
	KT111	Kiến thức về luật chứng cứ điện tử.						
	KT112	Kiến thức về các quy tắc pháp lý về chứng cứ và thủ tục tòa án.						
	KT117	Kiến thức về kỹ thuật quản trị hệ thống, mạng và cứng hóa (hardening) hệ điều hành.						
	KT118	Kiến thức về luật, nghị định, chỉ thị, quy định hiện hành về an toàn thông tin.						

Mã Tham chiếu	Mã Kiến thức	Kiến thức	Mã Kỹ năng	Kỹ năng	4	3	2	1
	KT127	Kiến thức về các khái niệm kiến trúc an toàn thông tin mạng bao gồm cấu trúc liên kết (topology), giao thức, các thành phần và nguyên tắc (ví dụ: phòng thủ chiều sâu defense-in-depth).						
	KT129	Kiến thức về các công cụ và kỹ thuật khôi phục dữ liệu.						
	KT130	Kiến thức về các khái niệm dịch ngược.						
	KT131	Kiến thức về các chiến thuật, kỹ thuật và quy trình chống điều tra số.						
	KT132	Kiến thức về cấu hình thiết kế phòng thí nghiệm điều tra và các ứng dụng hỗ trợ (ví dụ: VMWare, Wireshark).						
	KT133	Kiến thức về các quy trình và công cụ gỡ lỗi.						
	KT134	Kiến thức về các loại tệp tin có thể bị bên tấn công lợi dụng gây ra hành vi bất thường.						
	KT135	Kiến thức về các công cụ phân tích phần mềm mã độc (ví dụ: Oily Debug, Ida Pro).						
	KT136	Kiến thức về phần mềm độc hại với tính năng phát hiện máy ảo.						
	KT154	Kiến thức về các khái niệm quản trị hệ thống cho hệ điều hành, chẳng hạn như nhưng không giới hạn cho các hệ điều hành Unix/Linux, IOS, Android và Windows.						
	KT158	Kiến thức về phân tích nhị phân.						

Mã Tham chiếu	Mã Kiến thức	Kiến thức	Mã Kỹ năng	Kỹ năng	4	3	2	1
	KT159	Kiến thức về các khái niệm kiến trúc mạng bao gồm cấu trúc liên kết (topology), giao thức và các thành phần.						
	KT189	Kiến thức về phân tích gói tin bằng các công cụ thích hợp (ví dụ: Wireshark, tcpdump).						
	KT191	Kiến thức về các khái niệm và thực hành xử lý dữ liệu điều tra số.						
	KT210	Kiến thức và hiểu biết về thiết kế vận hành.						
	KT248	Kiến thức về rủi ro bảo mật ứng dụng (ví dụ: Danh sách top 10 lỗ hổng owasp).						
CSSS 7	**Nghiên cứu phát triển**					**x**	**x**	**x**
	KT001	Kiến thức về các khái niệm và giao thức mạng máy tính và phương pháp luận về an toàn thông tin mạng.	KN003	Kỹ năng ứng dụng và kết hợp công nghệ thông tin vào các giải pháp được đề xuất.				
	KT002	Kiến thức về các quy trình quản lý rủi ro (ví dụ: các phương pháp đánh giá và giảm thiểu rủi ro).	KN007	Kỹ năng tạo và sử dụng các mô hình toán học hoặc thống kê.				
	KT003	Kiến thức về luật, quy định, chính sách và đạo đức nghề nghiệp liên quan đến an toàn thông tin mạng và quyền riêng tư.	KN037	Kỹ năng sử dụng các quy tắc và phương pháp khoa học để giải quyết vấn đề.				
	KT004	Kiến thức về an toàn thông tin mạng và các nguyên tắc quyền riêng tư.	KN078	Kỹ năng áp dụng quy trình kỹ thuật hệ thống.				
	KT005	Kiến thức về các mối đe dọa và điểm yếu an toàn thông tin mạng.	KN082	Kỹ năng thiết kế tích hợp các quy trình và giải pháp công nghệ, bao gồm các hệ thống kế thừa và các ngôn ngữ lập trình hiện đại.				

Mã Tham chiếu	Mã Kiến thức	Kiến thức	Mã Kỹ năng	Kỹ năng	4	3	2	1
	KT006	Kiến thức về các ảnh hưởng đối với hoạt động do mất an toàn thông tin mạng.	KN091	Kỹ năng áp dụng các kỹ thuật lập trình an toàn.				
	KT009	Kiến thức về các điểm yếu ứng dụng.						
	KT018	Kiến thức về mật mã và các khái niệm quản lý khóa mật mã.						
	KT051	Kiến thức về các công nghệ mới và mới nổi lĩnh vực công nghệ thông tin và an toàn thông tin mạng.						
	KT075	Kiến thức về các nguyên tắc quản lý vòng đời hệ thống, bao gồm bảo mật phần mềm và khả năng sử dụng.						
	KT099	Kiến thức về thực hành Quản lý rủi ro chuỗi cung ứng.						
	KT119	Kiến thức về an toàn chuỗi cung ứng công nghệ thông tin và rủi ro chuỗi cung ứng, các chính sách, yêu cầu và thủ tục quản lý.						
	KT120	Kiến thức về các hệ thống hạ tầng quan trọng với công nghệ thông tin và truyền thông được thiết kế không quan tâm về bảo mật hệ thống.						
	KT121	Kiến thức về kỹ thuật dịch ngược phần cứng.						
	KT122	Kiến thức về phần mềm trung gian (middleware).						
	KT123	Kiến thức về các giao thức mạng.						
	KT124	Kiến thức về kỹ thuật dịch ngược phần mềm.						
	KT125	Kiến thức về tiêu chuẩn lược đồ XML.						

Mã Tham chiếu	Mã Kiến thức	Kiến thức	Mã Kỹ năng	Kỹ năng	4	3	2	1
	KT127	Kiến thức về các khái niệm kiến trúc an toàn thông tin mạng bao gồm cấu trúc liên kết (topology), giao thức, các thành phần và nguyên tắc (ví dụ: phòng thủ chiều sâu defense-in-depth).						
	KT143	Kiến thức về các khái niệm và chức năng của tường lửa ứng dụng.						
	KT147	Kiến thức về kỹ thuật che dấu kết nối.						
	KT169	Kiến thức về luật pháp, chính sách, thủ tục hoặc quản trị an toàn thông tin mạng cho các hạ tầng quan trọng.						
	KT170	Kiến thức về nhận dạng điều tra số.						
	KT171	Kiến thức về kiến trúc truyền thông di động.						
	KT172	Kiến thức về cấu trúc và nội bộ của hệ điều hành (ví dụ: quản lý quy trình, cấu trúc thư mục, các ứng dụng đã cài đặt).						
	KT173	Kiến thức về các công cụ phân tích mạng được sử dụng để xác định các điểm yếu phần mềm liên lạc.						
	KT183	Kiến thức về các tiêu chuẩn mô hình đảm bảo an toàn thông tin.						
	KT187	Kiến thức về khả năng, ứng dụng và các điểm yếu tiềm ẩn của thiết bị mạng, bao gồm các hub, bộ định tuyến, bộ chuyển mạch, cầu nối, máy chủ, phương tiện truyền dẫn và các phần cứng.						
	KT193	Kiến thức về các phương pháp hack.						

Mã Tham chiếu	Mã Kiến thức	Kiến thức	Mã Kỹ năng	Kỹ năng	4	3	2	1
	KT194	Kiến thức về các điểm yếu an toàn thông tin mạng tiềm ẩn của các công nghệ chuyên ngành.						
	KT197	Kiến thức về các khái niệm kỹ thuật được áp dụng cho kiến trúc máy tính và phần cứng/phần mềm máy tính liên quan.						
	KT208	Kiến thức về các nguyên tắc, công cụ và kỹ thuật kiểm thử xâm nhập.						
	KT235	Kiến thức về an toàn hoạt động.						
CSSS 8	**Đánh giá an toàn phần mềm**				**x**	**x**	**x**	**x**
	KT001	Kiến thức về các khái niệm và giao thức mạng máy tính và phương pháp luận về an toàn thông tin mạng.	KN001	Kỹ năng tiến hành rà quét điểm yếu và nhận biết các điểm yếu để đảm bảo an toàn các hệ thống.				
	KT002	Kiến thức về các quy trình quản lý rủi ro (ví dụ: các phương pháp đánh giá và giảm thiểu rủi ro).	KN009	Kỹ năng thiết kế các biện pháp đối phó với các rủi ro an toàn thông tin đã xác định.				
	KT003	Kiến thức về luật, quy định, chính sách và đạo đức nghề nghiệp liên quan đến an toàn thông tin mạng và quyền riêng tư.	KN014	Kỹ năng phát triển và áp dụng các biện pháp kiểm soát an toàn truy cập hệ thống.				
	KT004	Kiến thức về an toàn thông tin mạng và các nguyên tắc quyền riêng tư.	KN016	Kỹ năng xác định nhu cầu bảo vệ (ví dụ: các kiểm soát an toàn) của hệ thống thông tin và mạng.				
	KT005	Kiến thức về các mối đe dọa và điểm yếu an toàn thông tin mạng.	KN047	Kỹ năng tích hợp các công cụ kiểm tra an toàn thông tin hộp đen (black box) vào quy trình đảm bảo chất lượng của phát hành phần mềm.				

Mã Tham chiếu	Mã Kiến thức	Kiến thức	Mã Kỹ năng	Kỹ năng	4	3	2	1
	KT006	Kiến thức về các ảnh hưởng đối với hoạt động do mất an toàn thông tin mạng.	KN073	Kỹ năng xây dựng kế hoạch kiểm thử an toàn thông tin (ví dụ: kiểm thử đơn vị (unit test), kiểm thử tích hợp, kiểm thử hệ thống, kiểm thử chấp nhận (acceptance test)).				
	KT014	Kiến thức về cấu trúc dữ liệu phức tạp.	KN076	Kỹ năng sử dụng mã hóa hạ tầng khóa công khai (PKI) và chữ ký số vào các ứng dụng (ví dụ: email S/MIME, SSL).				
	KT016	Kiến thức về nguyên lý lập trình máy tính.	KN093	Kỹ năng sử dụng các công cụ phân tích dòng lệnh (code).				
	KT022	Kiến thức về kiến trúc an toàn thông tin của tổ chức.	KN094	Kỹ năng thực hiện phân tích nguyên nhân gốc.				
	KT023	Kiến thức về các yêu cầu đánh giá và xác nhận của tổ chức.	KN147	Kỹ năng áp dụng các nguyên tắc an toàn thông tin mạng và quyền riêng tư đối với các yêu cầu của tổ chức (liên quan đến tính bí mật, tính toàn vẹn, tính khả dụng, xác thực, chống chối bỏ).				
	KT033	Kiến thức về các nguyên tắc và phương pháp an toàn thông tin mạng và riêng tư áp dụng cho phát triển phần mềm.						
	KT038	Kiến thức về các nguyên tắc và yêu cầu an toàn thông tin mạng và riêng tư (liên quan đến tính bí mật, tính toàn vẹn, tính khả dụng, xác thực, chống chối bỏ).						
	KT043	Kiến thức về các nguyên tắc và khái niệm mạng nội bộ (LAN) và mạng diện rộng (WAN) bao gồm quản lý băng thông.						

Mã Tham chiếu	Mã Kiến thức	Kiến thức	Mã Kỹ năng	Kỹ năng	4	3	2	1
	KT044	Kiến thức về ngôn ngữ máy tính cấp thấp (ví dụ: hợp ngữ).						
	KT052	Kiến thức về hệ điều hành.						
	KT057	Kiến thức về Đánh giá tác động quyền riêng tư.						
	KT059	Kiến thức về cấu trúc ngôn ngữ lập trình và logic.						
	KT060	Kiến thức về các mối đe dọa và điểm yếu của hệ thống và ứng dụng (ví dụ: tràn bộ đệm (buffer overflow), mã di động (mobile code), cross-site scripting, PL/SQL injection, mã độc,...).						
	KT062	Kiến thức về kỹ thuật quản lý cấu hình an toàn.						
	KT067	Kiến thức về nguyên tắc gỡ lỗi phần mềm.						
	KT068	Kiến thức về các công cụ, phương pháp và kỹ thuật thiết kế phần mềm.						
	KT069	Kiến thức về các mô hình phát triển phần mềm (ví dụ: Mô hình thác nước - Waterfall, Mô hình xoắn ốc - Spiral Model).						
	KT070	Kiến thức về kỹ thuật phần mềm.						
CSSS 9	**Kiến trúc an toàn thông tin**					**x**	**x**	**x**
	KT001	Kiến thức về các khái niệm và giao thức mạng máy tính và phương pháp luận về an toàn thông tin mạng.	KN003	Kỹ năng ứng dụng và kết hợp công nghệ thông tin vào các giải pháp được đề xuất.				

Mã Tham chiếu	Mã Kiến thức	Kiến thức	Mã Kỹ năng	Kỹ năng	4	3	2	1
	KT002	Kiến thức về các quy trình quản lý rủi ro (ví dụ: các phương pháp đánh giá và giảm thiểu rủi ro).	KN009	Kỹ năng thiết kế các biện pháp đối phó với các rủi ro an toàn thông tin đã xác định				
	KT003	Kiến thức về luật, quy định, chính sách và đạo đức nghề nghiệp liên quan đến an toàn thông tin mạng và quyền riêng tư.	KN011	Kỹ năng thiết kế tích hợp các giải pháp phần cứng và phần mềm.				
	KT004	Kiến thức về an toàn thông tin mạng và các nguyên tắc quyền riêng tư.	KN013	Kỹ năng xác định cách thức hoạt động của hệ thống bảo mật (bao gồm khả năng phục hồi và khả năng tin cậy) và những thay đổi về điều kiện, hoạt động hoặc môi trường sẽ ảnh hưởng như thế nào đến những kết quả này.				
	KT005	Kiến thức về các mối đe dọa và điểm yếu an toàn thông tin mạng.	KN021	Kỹ năng thiết kế mô hình và xây dựng use case (ví dụ: Ngôn ngữ mô hình hóa thống nhất UML).				
	KT006	Kiến thức về các ảnh hưởng đối với hoạt động do mất an toàn thông tin mạng.	KN027	Kỹ năng sử dụng thiết bị Mạng riêng ảo (VPN) và mã hóa.				
	KT007	Kiến thức về phương pháp xác thực, ủy quyền và kiểm soát truy cập.	KN029	Kỹ năng viết kế hoạch kiểm tra/ kiểm thử.				
	KT008	Kiến thức về áp dụng các quy trình kinh doanh và hoạt động của các tổ chức.	KN041	Kỹ năng cài, thiết lập đặt cấu hình các phần mềm, công cụ bảo vệ máy tính. (ví dụ: phần mềm tường lửa, phần mềm chống vi-rút, phần mềm chống gián điệp).				
	KT009	Kiến thức về các điểm yếu ứng dụng.	KN063	Kỹ năng thiết kế các giải pháp an toàn đa lớp/liên miền (cross-domain).				
	KT010	Kiến thức về các phương pháp kết nối, nguyên tắc và khái niệm hạ tầng mạng.	KN066	Kỹ năng sử dụng các phương pháp thiết kế.				

Mã Tham chiếu	Mã Kiến thức	Kiến thức	Mã Kỹ năng	Kỹ năng	4	3	2	1
	KT011	Kiến thức về khả năng và ứng dụng của thiết bị mạng bao gồm bộ định tuyến (router), thiết bị chuyển mạch (switch), cầu nối (bridge), máy chủ, phương tiện truyền dẫn và phần cứng liên quan.	KN076	Kỹ năng sử dụng mã hóa hạ tầng khóa công khai (PKI) và chữ ký số vào các ứng dụng (ví dụ: email S/MIME, SSL).				
	KT012	Kiến thức về phân tích khả năng và yêu cầu.	KN077	Kỹ năng áp dụng các mô hình bảo mật (ví dụ: mô hình Bell-LaPadula, mô hình toàn vẹn Biba, mô hình toàn vẹn Clark Wilson).				
	KT013	Kiến thức về các công cụ bảo vệ và đánh giá điểm yếu an toàn thông tin mạng và khả năng của các công cụ.	KN083	Kỹ năng chuyển các yêu cầu nghiệp vụ thành nhu cầu bảo vệ (ví dụ: các biện pháp kiểm soát an ninh).				
	KT015	Kiến thức về thuật toán máy tính.	KN087	Kỹ năng thiết lập mạng con (subnet) vật lý hoặc logic để tách mạng cục bộ (LAN) khỏi các mạng không đáng tin cậy khác.				
	KT017	Kiến thức về các thuật toán mã hóa	KN089	Kỹ năng cấu hình và sử dụng các thành phần bảo vệ máy tính (ví dụ: tường lửa, máy chủ, bộ định tuyến, nếu thích hợp).				
	KT020	Kiến thức về hệ thống cơ sở dữ liệu.						
	KT021	Kiến thức về kế hoạch duy trì hoạt động và khôi phục thảm họa.						
	KT022	Kiến thức về kiến trúc an toàn thông tin của tổ chức.						
	KT025	Kiến thức về kỹ thuật, kiến trúc máy tính (ví dụ: bảng mạch, bộ xử lý, chip và phần cứng máy tính).						
	KT029	Kiến thức về cài đặt, tích hợp và tối ưu hóa các thành phần hệ thống thông tin.						

Mã Tham chiếu	Mã Kiến thức	Kiến thức	Mã Kỹ năng	Kỹ năng	4	3	2	1
	KT030	Kiến thức về nguyên lý tương tác giữa người và máy tính.						
	KT031	Kiến thức về quy trình Đánh giá và Ủy quyền bảo mật an toàn thông tin mạng.						
	KT037	Kiến thức về các nguyên tắc phân tích tiêu chuẩn ngành và các phương pháp được chấp nhận, áp dụng.						
	KT038	Kiến thức về các nguyên tắc và yêu cầu an toàn thông tin mạng và riêng tư (liên quan đến tính bí mật, tính toàn vẹn, tính khả dụng, xác thực, chống chối bỏ).						
	KT045	Kiến thức về toán học (ví dụ: logarit, lượng giác, đại số tuyến tính, giải tích, thống kê và phân tích hoạt động).						
	KT047	Kiến thức về vi xử lý (microprocessors) .						
	KT048	Kiến thức về truy cập mạng, danh tính và quản lý truy cập (ví dụ: hạ tầng khóa công khai, Oauth, OpenID, SAML, SPML).						
	KT049	Kiến thức về các thiết bị và chức năng phần cứng mạng.						
	KT051	Kiến thức về các công nghệ mới và mới nổi lĩnh vực công nghệ thông tin và an toàn thông tin mạng.						
	KT052	Kiến thức về hệ điều hành.						

Mã Tham chiếu	Mã Kiến thức	Kiến thức	Mã Kỹ năng	Kỹ năng	4	3	2	1
	KT053	Kiến thức về cách lưu lượng truyền qua mạng (ví dụ: Giao thức TCP, IP, Mô hình OSI,...).						
	KT055	Kiến thức về các khái niệm tính toán song song và phân tán.						
	KT061	Kiến thức về các khái niệm công nghệ truy cập từ xa.						
	KT063	Kiến thức về các khái niệm chính trong quản lý bảo mật an toàn thông tin mạng (ví dụ: Quản lý phát hành, Quản lý bản vá).						
	KT070	Kiến thức về kỹ thuật phần mềm.						
	KT076	Kiến thức về các phương pháp kiểm tra và đánh giá hệ thống.						
	KT077	Kiến thức về các quy trình tích hợp công nghệ.						
	KT078	Kiến thức về các khái niệm viễn thông (ví dụ: Kênh truyền, đa kênh,...).						
	KT082	Kiến thức về quy trình kỹ thuật hệ thống.						
	KT120	Kiến thức về các hệ thống hạ tầng quan trọng với công nghệ thông tin và truyền thông được thiết kế không quan tâm về bảo mật hệ thống.						
	KT128	Kiến thức về các nguyên tắc, mô hình, phương pháp quản lý hệ thống mạng và các công cụ.						
	KT140	Kiến thức về các khái niệm cải tiến quy trình tổ chức và quy trình mô hình trưởng thành.						

Mã Tham chiếu	Mã Kiến thức	Kiến thức	Mã Kỹ năng	Kỹ năng	4	3	2	1
	KT142	Kiến thức về các khái niệm quản lý dịch vụ mạng và các tiêu chuẩn liên quan (ví dụ: tiêu chuẩn ITIL).						
	KT143	Kiến thức về các khái niệm và chức năng của tường lửa ứng dụng.						
	KT149	Kiến thức về các yêu cầu về tính bí mật, tính toàn vẹn và tính khả dụng.						
	KT150	Kiến thức về các sản phẩm phần mềm hỗ trợ an toàn thông tin mạng.						
	KT151	Kiến thức về phương pháp đánh giá Khung quản lý rủi ro.						
	KT155	Kiến thức về các loại kiến trúc máy tính.						
	KT157	Kiến thức về giải pháp hệ thống bảo mật đa cấp và trên các tên miền khác nhau.						
	KT162	Kiến thức về các tiêu chuẩn an toàn thông tin cá nhân, dữ liệu cá nhân.						
	KT163	Kiến thức về các tiêu chuẩn an toàn dữ liệu thẻ thanh toán (PCI).						
	KT164	Kiến thức về các tiêu chuẩn an toàn dữ liệu thông tin y tế, sức khỏe cá nhân.						
	KT166	Kiến thức về lập kế hoạch chương trình bảo vệ (ví dụ: chính sách bảo mật chuỗi cung ứng/quản lý rủi ro, kỹ thuật chống giả mạo).						
	KT175	Kiến thức về kỹ thuật quản lý cấu hình.						

Mã Tham chiếu	Mã Kiến thức	Kiến thức	Mã Kỹ năng	Kỹ năng	4	3	2	1
	KT177	Kiến thức về mã hóa dữ liệu hiện tại và mới nổi, các tính năng bảo mật trong cơ sở dữ liệu (ví dụ: tích hợp sẵn tính năng quản lý khóa mật mã).						
	KT181	Kiến thức về N-tiered (ví dụ: bao gồm hệ điều hành máy chủ và máy khách).						
	KT182	Kiến thức về chương trình phân loại thông tin và các quy trình đối với xâm phạm thông tin.						
	KT185	Kiến thức về các khái niệm và mô hình kiến trúc công nghệ thông tin (ví dụ: đường cơ sở, xác nhận thiết kế và kiến trúc mục tiêu.)						
	KT186	Kiến thức về việc tích hợp các tầm nhìn và mục tiêu của tổ chức vào kiến trúc.						
	KT196	Kiến thức về các tiêu chí đánh giá và xác nhận của tổ chức.						
	KT198	Kiến thức về hệ thống nhúng.						
	KT199	Kiến thức về các phương pháp luận khả năng chịu lỗi của hệ thống.						
	KT201	Kiến thức về Lý thuyết thông tin (ví dụ: mã nguồn, mã hóa kênh, lý thuyết thuật toán phức tạp và nén dữ liệu).						
	KT202	Kiến thức về phân vùng DMZ.						
	KT203	Kiến thức về các giao thức mạng như TCP/IP, DHCP, DNS và các dịch vụ thư mục.						

Mã Tham chiếu	Mã Kiến thức	Kiến thức	Mã Kỹ năng	Kỹ năng	4	3	2	1
	KT204	Kiến thức về các quy trình thiết kế mạng, bao gồm hiểu biết về các mục tiêu bảo mật, mục tiêu nghiệp vụ và sự cân bằng.						
	KT206	Kiến thức về các phương pháp xác thực quyền truy cập.						
	KT241	Kiến thức về các giao thức mạng và định tuyến phổ biến (ví dụ: TCP/IP), các dịch vụ (ví dụ: web, thư, DNS) và cách chúng tương tác để cung cấp kết nối mạng.						
CSSS 10	**Triển khai an toàn hệ thống thông tin**					**x**	**x**	**x**
	KT001	Kiến thức về các khái niệm và giao thức mạng máy tính và phương pháp luận về an toàn thông tin mạng.	KN001	Kỹ năng tiến hành rà quét điểm yếu và nhận biết các điểm yếu để đảm bảo an toàn các hệ thống.				
	KT002	Kiến thức về các quy trình quản lý rủi ro (ví dụ: các phương pháp đánh giá và giảm thiểu rủi ro).	KN009	Kỹ năng thiết kế các biện pháp đối phó với các rủi ro an toàn thông tin đã xác định				
	KT003	Kiến thức về luật, quy định, chính sách và đạo đức nghề nghiệp liên quan đến an toàn thông tin mạng và quyền riêng tư.	KN010	Kỹ năng thiết kế các kiểm soát an toàn dựa trên nguyên tắc, nguyên lý an toàn thông tin mạng				
	KT004	Kiến thức về an toàn thông tin mạng và các nguyên tắc quyền riêng tư.	KN011	Kỹ năng thiết kế tích hợp các giải pháp phần cứng và phần mềm.				
	KT005	Kiến thức về các mối đe dọa và điểm yếu an toàn thông tin mạng.	KN014	Kỹ năng phát triển và áp dụng các biện pháp kiểm soát an toàn truy cập hệ thống.				
	KT006	Kiến thức về các ảnh hưởng đối với hoạt động do mất an toàn thông tin mạng	KN016	Kỹ năng xác định nhu cầu bảo vệ (ví dụ: các kiểm soát an toàn) của hệ thống thông tin và mạng.				
	KT015	Kiến thức về thuật toán máy tính.	KN017	Kỹ năng đánh giá tính đầy đủ của an toàn thiết kế.				

Mã Tham chiếu	Mã Kiến thức	Kiến thức	Mã Kỹ năng	Kỹ năng	4	3	2	1
	KT017	Kiến thức về các thuật toán mã hóa	KN048	Kỹ năng thực hiện đánh giá hoặc xem xét các hệ thống kỹ thuật.				
	KT020	Kiến thức về hệ thống cơ sở dữ liệu.	KN080	Kỹ năng tích hợp và áp dụng các chính sách để đáp ứng các mục tiêu an toàn hệ thống.				
	KT022	Kiến thức về kiến trúc an toàn thông tin của tổ chức.	KN085	Kỹ năng sử dụng mô hình thiết kế (ví dụ: Ngôn ngữ mô hình thống nhất UML).				
	KT023	Kiến thức về các yêu cầu đánh giá và xác nhận của tổ chức.	KN147	Kỹ năng áp dụng các nguyên tắc an toàn thông tin mạng và quyền riêng tư đối với các yêu cầu của tổ chức (liên quan đến tính bí mật, tính toàn vẹn, tính khả dụng, xác thực, chống chối bỏ).				
	KT025	Kiến thức về kỹ thuật, kiến trúc máy tính (ví dụ: bảng mạch, bộ xử lý, chip và phần cứng máy tính).						
	KT026	Kiến thức về khả năng phục hồi và dự phòng.						
	KT029	Kiến thức về cài đặt, tích hợp và tối ưu hóa các thành phần hệ thống thông tin						
	KT030	Kiến thức về nguyên lý tương tác giữa người và máy tính.						
	KT038	Kiến thức về các nguyên tắc và yêu cầu an toàn thông tin mạng và riêng tư (liên quan đến tính bí mật, tính toàn vẹn, tính khả dụng, xác thực, chống chối bỏ).						
	KT039	Kiến thức về các nguyên tắc kỹ thuật an toàn hệ thống thông tin.						

Mã Tham chiếu	Mã Kiến thức	Kiến thức	Mã Kỹ năng	Kỹ năng	4	3	2	1
	KT042	Kiến thức về các nguyên tắc và phương pháp an toàn thông tin (ví dụ: tường lửa, DMZ, mã hóa).						
	KT043	Kiến thức về các nguyên tắc và khái niệm mạng nội bộ (LAN) và mạng diện rộng (WAN) bao gồm quản lý băng thông.						
	KT045	Kiến thức về toán học (ví dụ: logarit, lượng giác, đại số tuyến tính, giải tích, thống kê và phân tích hoạt động).						
	KT047	Kiến thức về vi xử lý (microprocessors).						
	KT048	Kiến thức về truy cập mạng, danh tính và quản lý truy cập (ví dụ: hạ tầng khóa công khai, Oauth, OpenID, SAML, SPML).						
	KT052	Kiến thức về hệ điều hành.						
	KT053	Kiến thức về cách lưu lượng truyền qua mạng (ví dụ: Giao thức TCP, IP, Mô hình OSI,...).						
	KT055	Kiến thức về các khái niệm tính toán song song và phân tán.						
	KT056	Kiến thức về các biện pháp kiểm soát truy cập dựa trên chính sách và thích ứng với rủi ro.						
	KT057	Kiến thức về Đánh giá tác động quyền riêng tư.						
	KT058	Kiến thức về các khái niệm quy trình kỹ thuật.						
	KT062	Kiến thức về kỹ thuật quản lý cấu hình an toàn.						

Mã Tham chiếu	Mã Kiến thức	Kiến thức	Mã Kỹ năng	Kỹ năng	4	3	2	1
	KT069	Kiến thức về các mô hình phát triển phần mềm (ví dụ: Mô hình thác nước - Waterfall, Mô hình xoắn ốc - Spiral Model).						
	KT070	Kiến thức về kỹ thuật phần mềm.						
	KT071	Kiến thức về các nguyên tắc và phương pháp phân tích cấu trúc.						
	KT072	Kiến thức về các công cụ, phương pháp và kỹ thuật thiết kế hệ thống, bao gồm cả hệ thống tự động, các công cụ phân tích và thiết kế.						
	KT073	Kiến thức về hệ thống phần mềm và các tiêu chuẩn, chính sách thiết kế tổ chức và các phương pháp tiếp cận liên quan đến thiết kế hệ thống.						
	KT075	Kiến thức về các nguyên tắc quản lý vòng đời hệ thống, bao gồm bảo mật phần mềm và khả năng sử dụng.						
	KT076	Kiến thức về các phương pháp kiểm tra và đánh giá hệ thống.						
	KT078	Kiến thức về các khái niệm viễn thông (ví dụ: Kênh truyền, đa kênh,...).						
	KT082	Kiến thức về quy trình kỹ thuật hệ thống.						
	KT099	Kiến thức về thực hành Quản lý rủi ro chuỗi cung ứng.						
	KT106	Kiến thức về ngôn ngữ máy tính thông dịch và biên dịch.						

Mã Tham chiếu	Mã Kiến thức	Kiến thức	Mã Kỹ năng	Kỹ năng	4	3	2	1
	KT119	Kiến thức về an toàn chuỗi cung ứng công nghệ thông tin và rủi ro chuỗi cung ứng, các chính sách, yêu cầu và thủ tục quản lý.						
	KT120	Kiến thức về các hệ thống hạ tầng quan trọng với công nghệ thông tin và truyền thông được thiết kế không quan tâm về bảo mật hệ thống.						
	KT127	Kiến thức về các khái niệm kiến trúc an toàn thông tin mạng bao gồm cấu trúc liên kết (topology), giao thức, các thành phần và nguyên tắc (ví dụ: phòng thủ chiều sâu defense-in-depth).						
	KT128	Kiến thức về các nguyên tắc, mô hình, phương pháp quản lý hệ thống mạng và các công cụ.						
	KT142	Kiến thức về các khái niệm quản lý dịch vụ mạng và các tiêu chuẩn liên quan (ví dụ: tiêu chuẩn ITIL).						
	KT144	Kiến thức về các mô hình bảo mật (ví dụ: mô hình Bell-LaPadula, mô hình Biba, Mô hình Clark Wilson).						
	KT162	Kiến thức về các tiêu chuẩn an toàn thông tin cá nhân, dữ liệu cá nhân.						
	KT163	Kiến thức về các tiêu chuẩn an toàn dữ liệu thẻ thanh toán (PCI).						
	KT164	Kiến thức về các tiêu chuẩn an toàn dữ liệu thông tin y tế, sức khỏe cá nhân.						
	KT176	Kiến thức về quản lý an toàn thông tin.						

Mã Tham chiếu	Mã Kiến thức	Kiến thức	Mã Kỹ năng	Kỹ năng	4	3	2	1
	KT182	Kiến thức về chương trình phân loại thông tin và các quy trình đối với xâm phạm thông tin.						
	KT188	Kiến thức về thiết kế biện pháp đối phó với các rủi ro bảo mật đã xác định.						
	KT192	Kiến thức về mật mã học.						
	KT198	Kiến thức về hệ thống nhúng.						
	KT201	Kiến thức về Lý thuyết thông tin (ví dụ: mã nguồn, mã hóa kênh, lý thuyết thuật toán phức tạp và nén dữ liệu).						
	KT203	Kiến thức về các giao thức mạng như TCP/IP, DHCP, DNS và các dịch vụ thư mục.						
	KT204	Kiến thức về các quy trình thiết kế mạng, bao gồm hiểu biết về các mục tiêu bảo mật, mục tiêu nghiệp vụ và sự cân bằng.						
	KT206	Kiến thức về các phương pháp xác thực quyền truy cập.						
CSSS 11	**Vận hành an toàn hệ thống**					**x**	**x**	**x**
	KT001	Kiến thức về các khái niệm và giao thức mạng máy tính và phương pháp luận về an toàn thông tin mạng.	KN011	Kỹ năng thiết kế tích hợp các giải pháp phần cứng và phần mềm.				
	KT002	Kiến thức về các quy trình quản lý rủi ro (ví dụ: các phương pháp đánh giá và giảm thiểu rủi ro).	KN013	Kỹ năng xác định cách thức hoạt động của hệ thống bảo mật (bao gồm khả năng phục hồi và khả năng tin cậy) và những thay đổi về điều kiện, hoạt				

Mã Tham chiếu	Mã Kiến thức	Kiến thức	Mã Kỹ năng	Kỹ năng	4	3	2	1
				động hoặc môi trường sẽ ảnh hưởng như thế nào đến những kết quả này.				
	KT003	Kiến thức về luật, quy định, chính sách và đạo đức nghề nghiệp liên quan đến an toàn thông tin mạng và quyền riêng tư.	KN014	Kỹ năng phát triển và áp dụng các biện pháp kiểm soát an toàn truy cập hệ thống.				
	KT004	Kiến thức về an toàn thông tin mạng và các nguyên tắc quyền riêng tư.	KN017	Kỹ năng đánh giá tính đầy đủ của an toàn thiết kế.				
	KT005	Kiến thức về các mối đe dọa và điểm yếu an toàn thông tin mạng.	KN028	Kỹ năng viết mã bằng ngôn ngữ lập trình (ví dụ: Java, C++).				
	KT006	Kiến thức về các ảnh hưởng đối với hoạt động do mất an toàn thông tin mạng	KN079	Kỹ năng đánh giá an toàn thiết kế hệ thống.				
	KT015	Kiến thức về thuật toán máy tính.	KN081	Kỹ năng đánh giá các biện pháp kiểm soát an toàn dựa trên các nguyên tắc và nguyên lý an toàn thông tin mạng.				
	KT017	Kiến thức về các thuật toán mã hóa.	KN086	Kỹ năng nhận điểm yếu an toàn các hệ thống. (ví dụ: rà quét điểm yếu và xem xét sự tuân thủ).				
	KT018	Kiến thức về mật mã và các khái niệm quản lý khóa mật mã.	KN147	Kỹ năng áp dụng các nguyên tắc an toàn thông tin mạng và quyền riêng tư đối với các yêu cầu của tổ chức (liên quan đến tính bí mật, tính toàn vẹn, tính khả dụng, xác thực, chống chối bỏ).				
	KT020	Kiến thức về hệ thống cơ sở dữ liệu.						
	KT029	Kiến thức về cài đặt, tích hợp và tối ưu hóa các thành phần hệ thống thông tin.						

Mã Tham chiếu	Mã Kiến thức	Kiến thức	Mã Kỹ năng	Kỹ năng	4	3	2	1
	KT030	Kiến thức về nguyên lý tương tác giữa người và máy tính.						
	KT034	Kiến thức về các nguồn phổ biến thông tin về điểm yếu bảo mật (ví dụ: cảnh báo, tư vấn và bản tin,...).						
	KT038	Kiến thức về các nguyên tắc và yêu cầu an toàn thông tin mạng và riêng tư (liên quan đến tính bí mật, tính toàn vẹn, tính khả dụng, xác thực, chống chối bỏ).						
	KT042	Kiến thức về các nguyên tắc và phương pháp an toàn thông tin (ví dụ: tường lửa, DMZ, mã hóa).						
	KT045	Kiến thức về toán học (ví dụ: logarit, lượng giác, đại số tuyến tính, giải tích, thống kê và phân tích hoạt động).						
	KT048	Kiến thức về truy cập mạng, danh tính và quản lý truy cập (ví dụ: hạ tầng khóa công khai, Oauth, OpenID, SAML, SPML).						
	KT052	Kiến thức về hệ điều hành.						
	KT053	Kiến thức về cách lưu lượng truyền qua mạng (ví dụ: Giao thức TCP, IP, Mô hình OSI,...).						
	KT055	Kiến thức về các khái niệm tính toán song song và phân tán.						
	KT064	Kiến thức về các công cụ, phương pháp và kỹ thuật thiết kế hệ thống bảo mật.						

Mã Tham chiếu	Mã Kiến thức	Kiến thức	Mã Kỹ năng	Kỹ năng	4	3	2	1
	KT070	Kiến thức về kỹ thuật phần mềm.						
	KT078	Kiến thức về các khái niệm viễn thông (ví dụ: Kênh truyền, đa kênh,…).						
	KT082	Kiến thức về quy trình kỹ thuật hệ thống.						
	KT127	Kiến thức về các khái niệm kiến trúc an toàn thông tin mạng bao gồm cấu trúc liên kết (topology), giao thức, các thành phần và nguyên tắc (ví dụ: phòng thủ chiều sâu defense-in-depth).						
	KT128	Kiến thức về các nguyên tắc, mô hình, phương pháp quản lý hệ thống mạng và các công cụ.						
	KT142	Kiến thức về các khái niệm quản lý dịch vụ mạng và các tiêu chuẩn liên quan (ví dụ: tiêu chuẩn ITIL).						
	KT144	Kiến thức về các mô hình bảo mật (ví dụ: mô hình Bell-LaPadula, mô hình Biba, Mô hình Clark Wilson).						
	KT155	Kiến thức về các loại kiến trúc máy tính.						
	KT162	Kiến thức về các tiêu chuẩn an toàn thông tin cá nhân, dữ liệu cá nhân.						
	KT163	Kiến thức về các tiêu chuẩn an toàn dữ liệu thẻ thanh toán (PCI).						
	KT164	Kiến thức về các tiêu chuẩn an toàn dữ liệu thông tin y tế, sức khỏe cá nhân.						
	KT165	Kiến thức về các chính sách, yêu cầu và quy trình quản lý rủi ro công nghệ thông tin.						

Mã Tham chiếu	Mã Kiến thức	Kiến thức	Mã Kỹ năng	Kỹ năng	4	3	2	1
	KT168	Kiến thức về cách đánh giá mức độ đáng tin cậy của nhà cung cấp và /hoặc sản phẩm.						
	KT169	Kiến thức về luật pháp, chính sách, thủ tục hoặc quản trị an toàn thông tin mạng cho các hạ tầng quan trọng.						
	KT175	Kiến thức về kỹ thuật quản lý cấu hình.						
	KT176	Kiến thức về quản lý an toàn thông tin.						
	KT178	Kiến thức về danh mục dịch vụ công nghệ thông tin.						
	KT179	Kiến thức về phát triển và áp dụng hệ thống quản lý thông tin xác thực người dùng.						
	KT180	Kiến thức về triển khai hệ thống ký khóa để hỗ trợ dữ liệu ở trạng thái mã hóa nghỉ.						
	KT182	Kiến thức về chương trình phân loại thông tin và các quy trình đối với xâm phạm thông tin.						
	KT184	Kiến thức về các phương pháp kiểm tra và đánh giá bảo mật hệ thống.						
	KT188	Kiến thức về thiết kế biện pháp đối phó với các rủi ro bảo mật đã xác định.						
	KT198	Kiến thức về hệ thống nhúng.						
	KT204	Kiến thức về các quy trình thiết kế mạng, bao gồm hiểu biết về các mục tiêu bảo mật, mục tiêu nghiệp vụ và sự cân bằng.						
	KT207	Kiến thức về cách sử dụng các công cụ phân tích mạng để xác định các điểm yếu.						

Mã Tham chiếu	Mã Kiến thức	Kiến thức	Mã Kỹ năng	Kỹ năng	4	3	2	1
CSSS 12	**Phân tích/cảnh báo sớm**					x	x	x
	KT001	Kiến thức về các khái niệm và giao thức mạng máy tính và phương pháp luận về an toàn thông tin mạng.	KN098	Kỹ năng thực hiện nghiên cứu, tìm kiếm không theo quy trình (không xác định trước).				
	KT002	Kiến thức về các quy trình quản lý rủi ro (ví dụ: các phương pháp đánh giá và giảm thiểu rủi ro).	KN099	Kỹ năng thực hiện nghiên cứu bằng cách sử dụng web chìm (deep web).				
	KT003	Kiến thức về luật, quy định, chính sách và đạo đức nghề nghiệp liên quan đến an toàn thông tin mạng và quyền riêng tư.	KN100	Kỹ năng xác định và mô tả tất cả các khía cạnh thích hợp của môi trường hoạt động.				
	KT004	Kiến thức về an toàn thông tin mạng và các nguyên tắc quyền riêng tư.	KN101	Kỹ năng phát triển hoặc đề xuất các cách tiếp cận hoặc giải pháp phân tích cho các vấn đề và tình huống mà thông tin không đầy đủ hoặc chưa có tiền lệ.				
	KT005	Kiến thức về các mối đe dọa và điểm yếu an toàn thông tin mạng.	KN102	Kỹ năng đánh giá thông tin về độ tin cậy, tính hợp lệ và mức độ liên quan.				
	KT006	Kiến thức về các ảnh hưởng đối với hoạt động do mất an toàn thông tin mạng	KN103	Kỹ năng xác định các phân tích diễn giải thay thế nhằm giảm thiểu các kết quả không lường trước được.				
	KT030	Kiến thức về nguyên lý tương tác giữa người và máy tính.	KN104	Kỹ năng xác định thành phần mục tiêu quan trọng đối với không gian mạng.				
	KT050	Kiến thức về các phương pháp phân tích lưu lượng mạng.	KN105	Kỹ năng xác định các mối đe dọa mạng có thể gây nguy hiểm cho lợi ích của tổ chức và/hoặc đối tác.				

Mã Tham chiếu	Mã Kiến thức	Kiến thức	Mã Kỹ năng	Kỹ năng	4	3	2	1
	KT086	Kiến thức về các khái niệm, thuật ngữ và hoạt động của nhiều loại hình thông tin liên lạc phương tiện truyền thông (mạng máy tính và điện thoại, vệ tinh, cáp quang, không dây).	KN120	Kỹ năng chuẩn bị và trình bày các cuộc họp giao ban.				
	KT087	Kiến thức về các thành phần và kiến trúc máy tính vật lý, bao gồm các chức năng của các thành phần và thiết bị ngoại vi khác nhau (ví dụ: CPU, NIC, lưu trữ dữ liệu).	KN125	Kỹ năng cung cấp sự hiểu biết về các hệ thống mục tiêu hoặc mối đe dọa thông qua việc xác định và phân tích liên kết các mối quan hệ vật lý, chức năng hoặc hành vi.				
	KT126	Kiến thức về các giai đoạn tấn công mạng (ví dụ: trinh sát, dò quét, liệt kê, truy nhập hệ thống, leo thang đặc quyền, duy trì truy cập, khai thác mạng, xóa dấu vết).	KN128	Kỹ năng điều chỉnh phân tích theo các cấp độ cần thiết (ví dụ: phân loại và tổ chức).				
	KT211	Kiến thức về các loại trang web, quản trị, chức năng và hệ thống quản lý nội dung (CMS).	KN132	Kỹ năng sử dụng toán tử lôgic để xây dựng các truy vấn đơn giản và phức tạp.				
	KT212	Kiến thức về các phương pháp và kỹ thuật tấn công (DDoS, brute force, giả mạo, v.v.).	KN133	Kỹ năng sử dụng công cụ, cơ sở dữ liệu và kỹ thuật phân tích.				
	KT213	Kiến thức về tiêu chuẩn, chính sách và quy trình phân loại và và kiểm soát Mã ký hiệu.	KN134	Kỹ năng sử dụng công cụ tìm kiếm (ví dụ: Google, Yahoo, Baidu ..) và các công cụ tìm kiếm nguồn mở.				
	KT214	Kiến thức về các trường hợp phổ biến của lây nhiễm máy tính/mạng (virus, Trojan, v.v.) và các phương pháp lây nhiễm (cổng, tệp đính kèm, v.v.).	KN135	Kỹ năng sử dụng phản hồi để cải thiện quy trình, sản phẩm và dịch vụ.				
	KT215	Kiến thức về các nguyên tắc cơ bản về mạng máy tính (như: các thành phần cơ bản của mạng máy tính, các loại mạng, v.v.).	KN136	Kỹ năng sử dụng các công cụ / không gian làm việc cộng tác ảo).				

Mã Tham chiếu	Mã Kiến thức	Kiến thức	Mã Kỹ năng	Kỹ năng	4	3	2	1
	KT216	Kiến thức về các bộ xâm nhập trên máy tính hiện hành.	KN137	Kỹ năng viết báo cáo, xem xét và chỉnh sửa các sản phẩm đánh giá/thu thập thông tin liên quan đến không gian mạng từ nhiều nguồn.				
	KT217	Kiến thức về khả năng thu thập thông tin/trinh sát mạng và lưu trữ.						
	KT218	Kiến thức về thuật ngữ/từ vựng hoạt động an toàn thông tin mạng.						
	KT219	Kiến thức về thuật ngữ kết nối dữ liệu (ví dụ: giao thức mạng, Ethernet, IP, mã hóa, thiết bị quang, phương tiện di động).						
	KT220	Kiến thức về các thuật toán mã hóa và các khả năng/công cụ (ví dụ: SSL, PGP).						
	KT221	Kiến thức về các công nghệ truyền thông đang phát triển / mới nổi.						
	KT222	Kiến thức về các khái niệm hoạt động cơ bản về an toàn thông tin mạng, thuật ngữ/từ vựng (ví dụ: chuẩn bị môi trường, tấn công mạng, phòng thủ mạng), nguyên tắc, khả năng, giới hạn và tác động.						
	KT223	Kiến thức chung về các thành phần Hệ thống Điều khiển giám sát và thu thập dữ liệu (SCADA).						
	KT224	Kiến thức về các sản phẩm an toàn thông tin trên máy chủ và cách các sản phẩm đó ảnh hưởng đến việc khai thác và giảm điểm yếu.						
	KT225	Kiến thức về cách hoạt động của các ứng dụng Internet (SMTP email, web-based email, chat clients, VOIP).						

Mã Tham chiếu	Mã Kiến thức	Kiến thức	Mã Kỹ năng	Kỹ năng	4	3	2	1
	KT226	Kiến thức về cách thức các mạng điện thoại và kỹ thuật số hiện đại tác động đến hoạt động an toàn thông tin mạng.						
	KT227	Kiến thức về cách thức các hệ thống truyền thông không dây hiện đại tác động đến các hoạt động an toàn thông tin mạng.						
	KT228	Kiến thức về cách trích xuất, phân tích và sử dụng siêu dữ liệu.						
	KT229	Kiến thức về các kỹ luật trong hoạt động trinh sát.						
	KT230	Kiến thức về sự chuẩn bị trinh sát của môi trường và các quá trình tương tự.						
	KT231	Kiến thức về hỗ trợ trinh sát như lập kế hoạch, thực hiện và đánh giá.						
	KT232	Kiến thức về các chiến thuật nội bộ để dự đoán và/hoặc mô phỏng các khả năng và hành động của mối đe dọa.						
	KT233	Kiến thức về địa chỉ mạng Internet (địa chỉ IP, định tuyến liên miền không phân lớp, đánh số cổng TCP/UDP).						
	KT234	Kiến thức về mã độc.						
	KT235	Kiến thức về an toàn hoạt động.						
	KT236	Kiến thức về hệ thống phân cấp tổ chức và quy trình ra quyết định.						

Mã Tham chiếu	Mã Kiến thức	Kiến thức	Mã Kỹ năng	Kỹ năng	4	3	2	1
	KT237	Kiến thức về các thiết bị và hạ tầng mạng vật lý và logic, bao gồm hubs, bộ định tuyến (router), thiết bị chuyển mạch (switch), tường lửa (firewalls), v.v.						
	KT238	Kiến thức cơ bản về viễn thông.						
	KT239	Kiến thức về cấu trúc cơ bản, kiến trúc và thiết kế của mạng thông tin hiện đại.						
	KT240	Kiến thức cơ bản về bảo mật mạng (ví dụ: mã hóa, tường lửa, xác thực, honeypots, bảo vệ vùng biên).						
	KT241	Kiến thức về các giao thức mạng và định tuyến phổ biến (ví dụ: TCP/IP), các dịch vụ (ví dụ: web, thư, DNS) và cách chúng tương tác để cung cấp kết nối mạng.						
	KT242	Kiến thức về các cách mà các mục tiêu hoặc mối đe dọa sử dụng Internet.						
	KT243	Kiến thức về các mối đe dọa và/hoặc các hệ thống mục tiêu.						
	KT244	Kiến thức về các sản phẩm ảo hóa (VMware, Virtual PC).						
	KT245	Kiến thức về những cấu thành của "mối đe dọa" đối với mạng.						
	KT246	Kiến thức về các công nghệ không dây (ví dụ: di động, vệ tinh, GSM) bao gồm cấu trúc cơ bản, kiến trúc và thiết kế của các hệ thống không dây hiện đại.						