SAO Y; Bộ thông tin và Truyền thông; 26/09/2022 16:06:11

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

THÔNG TƯ
Quy định chuẩn kỹ năng nhân lực công nghệ thông tin chuyên nghiệp

Thông tư số 11/2015/TT-BTTTT ngày 05 tháng 5 năm 2015 của Bộ trưởng Bộ Thông tin và Truyền thông quy định chuẩn kỹ năng nhân lực công nghệ thông tin chuyên nghiệp, có hiệu lực kể từ ngày 22 tháng 6 năm 2015 được sửa đổi, bổ sung bởi:

Thông tư số 17/2021/TT-BTTTT ngày 30 tháng 11 năm 2021 của Bộ trưởng Bộ Thông tin và Truyền thông 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, có hiệu lực kể từ ngày 01 tháng 6 năm 2022.

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

Căn cứ Nghị định số 132/2013/NĐ-CP ngày 16 tháng 10 năm 2013 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 Vụ trưởng Vụ Công nghệ thông tin,

Bộ trưởng Bộ Thông tin và Truyền thông ban hành Thông tư Quy định Chuẩn kỹ năng nhân lực công nghệ thông tin chuyên nghiệp[1].

---

[1] Thông tư số 17/2021/TT-BTTTT ngày 30 tháng 11 năm 2021 của Bộ trưởng Bộ Thông tin và Truyền thông 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, có hiệu lực kể từ ngày 01 tháng 6 năm 2022 có căn cứ ban hành như sau:
"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. Phạm vi điều chỉnh

Thông tư này quy định một số Chuẩn kỹ năng nhân lực công nghệ thông tin chuyên nghiệp, bao gồm:

1. Chuẩn kỹ năng Cơ sở dữ liệu (Database skill standard);

2. Chuẩn kỹ năng Hệ thống mạng (Network system skill standard);

3. Chuẩn kỹ năng Quản lý hệ thống công nghệ thông tin (System management skill standard);

4.[2] Chuẩn kỹ năng An toàn thông tin (Cybersecurity Skill Standard);

5. Chuẩn kỹ năng Thiết kế và phát triển phần mềm (Software design and development skill standard).

Điều 2. Đối tượng áp dụng

1. Thông tư này áp dụng đối với cơ quan, tổ chức, cá nhân tham gia trực tiếp hoặc có liên quan đến việc đánh giá kỹ năng chuyên ngành của nhân lực công nghệ thông tin (CNTT), trong hoạt động đào tạo ngắn hạn, bồi dưỡng các kỹ năng chuyên ngành.

2. Khuyến khích các tổ chức, cá nhân áp dụng Thông tư này trong việc xây dựng chương trình, giáo trình đào tạo; tuyển dụng, sử dụng lao động; học tập, nâng cao trình độ và các hoạt động khác liên quan đến việc đánh giá trình độ, kỹ năng chuyên môn của nhân lực CNTT.

Điều 3. Giải thích từ ngữ

Trong văn bản này, các từ ngữ dưới đây được hiểu như sau:

1.[3] 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

---

[2] Khoản này được sửa đổi, bổ sung theo quy định tại khoản 1 Điều 1 của Thông tư số 17/2021/TT-BTTTT ngày 30 tháng 11 năm 2021 của Bộ trưởng Bộ Thông tin và Truyền thông 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, có hiệu lực kể từ ngày 01 tháng 6 năm 2022.

[3] Khoản này được sửa đổi, bổ sung theo quy định tại khoản 2 Điều 1 của Thông tư số 17/2021/TT-BTTTT ngày 30 tháng 11 năm 2021 của Bộ trưởng Bộ Thông tin và Truyền thông 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, có hiệu lực kể từ ngày 01 tháng 6 năm 2022.

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.

2. Trình độ trung cấp, cao đẳng, đại học sử dụng trong việc xếp hạng chuẩn kỹ năng quy định tại Điều 4 Thông tư này là các mức độ kiến thức được quy định tại Luật Giáo dục và các văn bản hướng dẫn thi hành.

Điều 4. Quy định Chuẩn kỹ năng nhân lực CNTT chuyên nghiệp

1. Chuẩn kỹ năng nhân lực CNTT chuyên nghiệp là hệ thống các yêu cầu về kiến thức và kỹ năng CNTT mà người làm việc trong lĩnh vực CNTT cần đạt để có thể thực hiện một hoặc một nhóm công việc cụ thể. Một số Chuẩn kỹ năng nhân lực CNTT chuyên nghiệp như sau:

a) Chuẩn kỹ năng Cơ sở dữ liệu (Mã DBSS): gồm các yêu cầu về kiến thức và kỹ năng cần thiết để thực hiện những công việc liên quan đến các hoạt động xây dựng kế hoạch tổng thể, xác định yêu cầu, phân tích, thiết kế, xây dựng, thử nghiệm và quản lý vận hành hệ thống cơ sở dữ liệu.

b) Chuẩn kỹ năng Hệ thống mạng (Mã NWSS): gồm các yêu cầu về kiến thức và kỹ năng cần thiết để thực hiện những công việc liên quan đến các hoạt động xác định yêu cầu, thiết kế, xây dựng, thử nghiệm, vận hành, bảo trì, quản lý và tư vấn phát triển hệ thống mạng máy tính.

c) Chuẩn kỹ năng Quản lý hệ thống CNTT (Mã SMSS): gồm các yêu cầu về kiến thức và kỹ năng cần thiết để thực hiện những công việc liên quan đến các hoạt động lập kế hoạch, quản lý vận hành, quản lý nhân lực, quản lý người sử dụng, quản lý tài nguyên, quản lý lỗi và sự cố, quản lý an toàn thông tin, quản lý hiệu năng, bảo trì, đánh giá hoạt động của hệ thống và hỗ trợ người sử dụng.

d)[4] 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.

đ) Chuẩn kỹ năng Thiết kế và phát triển phần mềm (Mã SDSS): gồm các yêu cầu về kiến thức và kỹ năng cần thiết để thực hiện những công việc liên quan đến các hoạt động xác định, phân tích yêu cầu người sử dụng, xác định yêu cầu hệ thống hóa, chuẩn bị phát triển hệ thống, thiết kế tổng thể, thiết kế thành phần, thiết kế chi tiết, lập trình, hỗ trợ cài đặt phần mềm và kiểm thử phần mềm.

2. Yêu cầu về kiến thức, kỹ năng: mỗi Chuẩn kỹ năng nhân lực CNTT chuyên nghiệp có yêu cầu về kiến thức cơ bản và yêu cầu về kiến thức, kỹ năng chuyên sâu. Cụ thể như sau:

---

[4] Điểm này được sửa đổi theo quy định tại khoản 3 Điều 1 của Thông tư số 17/2021/TT-BTTTT ngày 30 tháng 11 năm 2021 của Bộ trưởng Bộ Thông tin và Truyền thông 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, có hiệu lực kể từ ngày 01 tháng 6 năm 2022.

a) Yêu cầu kiến thức cơ bản: yêu cầu kiến thức cơ bản về CNTT đối với các Chuẩn kỹ năng nhân lực CNTT chuyên nghiệp được quy định tại Phụ lục số 01 Thông tư này, với trình độ tương ứng theo từng hạng quy định tại Khoản 3 Điều này.

b) Yêu cầu về kiến thức, kỹ năng chuyên sâu:

- Chuẩn kỹ năng Cơ sở dữ liệu: các yêu cầu về kiến thức, kỹ năng chuyên sâu của Chuẩn kỹ năng Cơ sở dữ liệu được quy định tại Phụ lục số 02 Thông tư này.

- Chuẩn kỹ năng Hệ thống mạng: các yêu cầu về kiến thức, kỹ năng chuyên sâu của Chuẩn kỹ năng Hệ thống mạng được quy định tại Phụ lục số 03 Thông tư này.

- Chuẩn kỹ năng Quản lý hệ thống CNTT: các yêu cầu về kiến thức, kỹ năng chuyên sâu của Chuẩn kỹ năng Quản lý hệ thống CNTT được quy định tại Phụ lục số 04 Thông tư này.

- 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[5].

- Chuẩn kỹ năng Thiết kế và phát triển phần mềm: các yêu cầu về kiến thức, kỹ năng chuyên sâu của Chuẩn kỹ năng Thiết kế và phát triển phần mềm được quy định tại Phụ lục số 06 Thông tư này.

3. Phân hạng các Chuẩn kỹ năng nhân lực CNTT chuyên nghiệp: mỗi Chuẩn kỹ năng nhân lực CNTT chuyên nghiệp được chia thành 4 hạng theo thứ tự từ thấp đến cao tương ứng hạng 04 đến hạng 01. Cụ thể như sau:

a) Hạng 4:

- Đáp ứng yêu cầu kiến thức cơ bản về CNTT quy định tại Điểm a, Khoản 02 Điều này ở trình độ trung cấp, hoặc tốt nghiệp ngành đào tạo về CNTT trình độ trung cấp, trung cấp nghề trở lên.

- Đáp ứng các mục yêu cầu về kiến thức, kỹ năng chuyên sâu của hạng 4 tương ứng với mỗi chuẩn theo quy định tại Điểm b, Khoản 2 Điều này.

b) Hạng 3:

- Đáp ứng yêu cầu kiến thức cơ bản về CNTT quy định tại Điểm a, Khoản 02 Điều này ở trình độ cao đẳng, hoặc tốt nghiệp ngành đào tạo về CNTT trình độ cao đẳng, cao đẳng nghề trở lên.

---

[5] 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" được thay thế bởi 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" theo quy định tại khoản 4 Điều 1 của Thông tư số 17/2021/TT-BTTTT ngày 30 tháng 11 năm 2021 của Bộ trưởng Bộ Thông tin và Truyền thông 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, có hiệu lực kể từ ngày 01 tháng 6 năm 2022.

- Đáp ứng các mục yêu cầu về kiến thức, kỹ năng chuyên sâu của hạng 3 tương ứng với mỗi chuẩn theo quy định tại Điểm b, Khoản 2 Điều này.

c) Hạng 2:

- Đáp ứng yêu cầu kiến thức cơ bản về CNTT quy định tại Điểm a, Khoản 02 Điều này ở trình độ đại học, hoặc tốt nghiệp ngành đào tạo về CNTT trình độ đại học trở lên.

- Đáp ứng các mục yêu cầu về kiến thức, kỹ năng chuyên sâu của hạng 2 tương ứng với mỗi chuẩn theo quy định tại Điểm b, Khoản 2 Điều này.

- Có khả năng phụ trách một nhóm cán bộ kỹ thuật từ 10 người trở lên thuộc lĩnh vực phù hợp với chuẩn kỹ năng tương ứng.

- Có thời gian làm công việc tương ứng 6 năm liên tục trở lên ở hạng 3.

d) Hạng 1:

- Đáp ứng yêu cầu kiến thức cơ bản về CNTT quy định tại Điểm a, Khoản 02 Điều này ở trình độ đại học, hoặc tốt nghiệp ngành đào tạo về CNTT trình độ đại học trở lên.

- Đáp ứng các mục yêu cầu về kiến thức, kỹ chuyên sâu của hạng 1 tương ứng với mỗi chuẩn theo quy định tại Điểm b, Khoản 2 Điều này.

- Có khả năng phụ trách một nhóm cán bộ kỹ thuật từ 50 người trở lên thuộc lĩnh vực phù hợp với chuẩn kỹ năng tương ứng.

- Có thời gian làm công việc tương ứng 3 năm liên tục trở lên ở hạng 2.

Điều 5. Hiệu lực thi hành[6]

Thông tư này có hiệu lực kể từ ngày 22 tháng 6 năm 2015.

Điều 6. Tổ chức thực hiện

1. Chánh văn phòng, Cục trưởng Cục An toàn thông tin, Cục trưởng Cục Công nghiệp công nghệ thông tin và Truyền thông, 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.

---

[6] Điều 4, Điều 5 của Thông tư số 17/2021/TT-BTTTT ngày 30 tháng 11 năm 2021 của Bộ trưởng Bộ Thông tin và Truyền thông 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, có hiệu lực kể từ ngày 01 tháng 6 năm 2022 quy định như sau:

*"**Điều 4. Điều khoản thi hành***

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

Điều 3. Tổ chức thực hiện

1. Chánh Văn phòng, Cục trưởng Cục An toàn thông tin, Cục trưởng Cục Công nghiệp công nghệ thông tin và Truyền thông, 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 Cục Công nghiệp công nghệ thông tin và Truyền thông tham mưu, hướng dẫn tổ chức thực hiện về Chuẩn kỹ năng An toàn thông tin."

2. Giao Cục Công nghiệp công nghệ thông tin và Truyền thông có trách nhiệm tham mưu, tổ chức hướng dẫn việc thực hiện Thông tư này; nghiên cứu, đề xuất, bổ sung, cập nhật các Chuẩn kỹ năng nhân lực CNTT chuyên nghiệp phù hợp với điều kiện thực tế.

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

3. Trong quá trình thực hiện, có phát sinh vướng mắc, cơ quan, tổ chức, cá nhân phản ánh về Bộ Thông tin và Truyền thông (Cục Công nghiệp công nghệ thông tin và Truyền thông) để kịp thời giải quyết./.

BỘ THÔNG TIN VÀ TRUYỀN THÔNG

Số: 12 /VBHN-BTTTT

XÁC THỰC VĂN BẢN HỢP NHẤT

Hà Nội, ngày 26 tháng 9 năm 2022

Nơi nhận:
- Văn phòng Chính phủ (để đăng Công báo và đăng tải trên Cổng TTĐT Chính phủ);
- Bộ TT&TT: Bộ trưởng và các Thứ trưởng; các cơ quan, đơn vị thuộc Bộ;
- Cổng TTĐT Bộ TT&TT (để đăng tải);
- Lưu: VT, CATTT, CNCNTT&TT (10b).

BỘ TRƯỞNG

Nguyễn Mạnh Hùng

PHỤ LỤC SỐ 01
YÊU CẦU KIẾN THỨC CƠ BẢN VỀ CNTT

(Ban hành kèm theo Thông tư số 11/2015/TT-BTTTT ngày 5/5/2015 của Bộ trưởng Bộ Thông tin và Truyền thông)

1	Lý thuyết cơ sở	1.1	Lý thuyết cơ sở	1.1.1	Toán rời rạc
				1.1.2	Toán ứng dụng
				1.1.3	Lý thuyết về thông tin
				1.1.4	Lý thuyết về truyền thông
				1.1.5	Lý thuyết về đo lường và điều khiển
		1.2	Thuật toán và lập trình	1.2.1	Cấu trúc dữ liệu
				1.2.2	Thuật toán
				1.2.3	Lập trình
				1.2.4	Các ngôn ngữ lập trình
2	Hệ thống máy tính	2.1	Các cấu phần máy tính	2.1.1	Bộ vi xử lý
				2.1.2	Bộ nhớ
				2.1.3	Bus
				2.1.4	Giao diện vào/ra
				2.1.5	Thiết bị vào/ra
		2.2	Các cấu phần hệ thống	2.2.1	Cấu hình hệ thống
				2.2.2	Các chỉ số đánh giá hệ thống
		2.3	Phần mềm	2.3.1	Hệ điều hành
				2.3.2	Phần mềm trung gian
				2.3.3	Hệ thống tệp
				2.3.4	Các công cụ phát triển
				2.3.5	Phần mềm nguồn mở
		2.4	Phần cứng	2.4.1	Phần cứng
3	Thành phần kỹ thuật	3.1	Giao diện người sử dụng	3.1.1	Công nghệ giao diện người sử dụng
				3.1.2	Thiết kế giao diện
		3.2	Đa phương tiện	3.2.1	Công nghệ đa phương tiện
				3.2.2	Ứng dụng đa phương tiện
		3.3	Cơ sở dữ liệu (CSDL)	3.3.1	Hệ thống CSDL
				3.3.2	Thiết kế CSDL
				3.3.3	Thao tác với dữ liệu
				3.3.4	Xử lý giao dịch (transaction processing)
				3.3.5	Ứng dụng CSDL
		3.4	Mạng	3.4.1	Kiến trúc mạng
				3.4.2	Truyền và điều khiển dữ liệu
				3.4.3	Các giao thức truyền tin
				3.4.4	Quản lý mạng
				3.4.5	Ứng dụng mạng
		3.5	Bảo mật	3.5.1	Bảo mật thông tin
				3.5.2	Quản lý bảo mật thông tin
				3.5.3	Đánh giá công nghệ bảo mật
				3.5.4	Đo lường bảo mật thông tin
				3.5.5	Công nghệ thực hiện bảo mật
4	...g ng hệ ph ...át	4.1	Công nghệ phát triển	4.1.1	Xác định các yêu cầu hệ thống

			hệ thống	4.1.2	Thiết kế kiến trúc hệ thống
				4.1.3	Xác định các yêu cầu phần mềm
				4.1.4	Thiết kế kiến trúc phần mềm và thiết kế chi tiết phần mềm
				4.1.5	Lập trình và kiểm thử phần mềm
				4.1.6	Tích hợp phần mềm và kiểm thử chất lượng phần mềm
				4.1.7	Tích hợp hệ thống và kiểm thử chất lượng hệ thống
				4.1.8	Cài đặt phần mềm
				4.1.9	Bàn giao phần mềm
				4.1.10	Bảo trì phần mềm
		4.2	Các kỹ thuật quản lý phát triển phần mềm	4.2.1	Quy trình và các phương pháp phát triển
				4.2.2	Quản lý về bản quyền phần mềm
				4.2.3	Quản lý môi trường phát triển
				4.2.4	Quản lý cấu hình và quản lý thay đổi

PHỤ LỤC SỐ 02
YÊU CẦU VỀ KIẾN THỨC, KỸ NĂNG CHUYÊN SÂU CỦA CHUẨN KỸ NĂNG CƠ SỞ DỮ LIỆU

(Ban hành kèm theo Thông tư số 11/2015/TT-BTTTT ngày 5/5/2015 của Bộ trưởng Bộ Thông tin và Truyền thông)

Mã tham chiếu	Nội dung/ Yêu cầu cần đạt		Yêu cầu cần đạt theo hạng			
	Kiến thức	Kỹ năng	4	3	2	1
DBSS 1	**Mô đun: Xây dựng kế hoạch tổng thể về cơ sở dữ liệu**				x	x
DBSS 1.1	Xây dựng kế hoạch về hệ thống CSDL					
	- Các phương pháp đánh giá hệ thống thông tin. - Các phương pháp phân tích vấn đề. - Việc bảo trì hệ CSDL	- Đánh giá việc sử dụng CSDL. - Đánh giá việc bảo trì CSDL. - Vận hành và quản lý CSDL. - Nghiên cứu tổng thể các hệ thống thông tin và CSDL. - Lập kế hoạch. - Sử dụng công cụ lập kế hoạch. - Giải thích rõ ràng về kế hoạch cho những người liên quan đến CSDL. - Đánh giá các yêu cầu cần đáp ứng của CSDL. - Thiết kế, xây dựng CSDL tuân thủ các tiêu chuẩn. - Đánh giá khối lượng và độ phức tạp của dữ liệu.				
DBSS 1.2	Chuẩn hóa CSDL					
	- Các thành phần dữ liệu. - Thiết kế mã. - Thiết kế dữ liệu. - Tính toàn vẹn của dữ liệu.	- Thiết lập các quy tắc về chuẩn dữ liệu. - Thiết kế mã. - Giải thích việc chuẩn hóa mã và dữ liệu cho những người phát triển ứng dụng. - Nhận biết và xử lý khi có các quan điểm khác nhau.				
DBSS 2	**Mô đun: Xác định yêu cầu của CSDL**			x	x	x
DBSS 2.1	Khảo sát hiện trạng và phân tích nhiệm vụ				x	x
	- Chi tiết công việc của người sử dụng. - Phương pháp thu thập thông tin. - Các phương pháp phân tích dữ liệu.	- Xác định nguồn tin về nhu cầu của người sử dụng. - Thực hiện các kỹ thuật và trình tự thu thập thông tin. - Xác định lượng thông tin cần thu thập.				

Mã tham chiếu	Nội dung/ Yêu cầu cần đạt		Yêu cầu cần đạt theo hạng			
	Kiến thức	Kỹ năng	4	3	2	1
	- Các phương pháp phân tích vấn đề.	- Phân tích câu trả lời của các cá nhân và các nhóm. - Lựa chọn, phân tích thông tin thu thập được và xác định nhu cầu. - Tập hợp và tóm tắt các thông tin đã yêu cầu. - Tổ chức thảo luận về các vấn đề quan trọng và đưa ra các giải pháp khác nhau.				
DBSS 2.2	Xác định phạm vi công việc					
	- Môi trường hệ thống. - Kiến trúc hệ thống, phần cứng và phần mềm. - Phát triển CSDL. - Tính sẵn sàng của các tài nguyên hệ thống và ngày bàn giao dự án. - Cách tính giờ công. - Các hạn chế kỹ thuật. - Các phương pháp phân tích rủi ro.	- Biên soạn tài liệu rõ ràng về phạm vi công việc đáp ứng các yêu cầu của người sử dụng. - Phân biệt quy mô, phạm vi và độ phức tạp của dự án. - Đàm phán với những người liên quan về các tiêu chí thành công của dự án CSDL. - Tính toán giờ công làm việc cho mỗi mục công việc của dự án CSDL. - Khảo sát, phân tích và so sánh các sản phẩm trên thị trường để xác định khả năng áp dụng cho dự án. - Lập tài liệu về các hạn chế kỹ thuật. - Tư duy tổng thể.				
DBSS 2.3	Xác định yêu cầu sơ bộ của CSDL					
	- Môi trường phát triển hệ thống và môi trường vận hành hệ thống. - CSDL và tích hợp công việc. - Chức năng và hoạt động của hệ thống. - Thiết kế và vận hành CSDL. - Phân tích dữ liệu. - Xác định các yêu cầu hiệu năng hệ thống. - Chính sách an toàn thông tin của tổ chức. - Đảm bảo toàn vẹn dữ liệu. - Kiểm soát truy cập dữ liệu.	- Chuyển đổi yêu cầu của người sử dụng thành các yêu cầu của CSDL. - Nhận biết các yêu cầu mâu thuẫn nhau và đưa ra các giải pháp. - Phân tích sự chính xác và nhất quán của thông tin. - Áp dụng công nghệ hiệu quả đáp ứng các yêu cầu. - Tìm hiểu về sự phân tán của dữ liệu - Đánh giá các tiêu chí đánh giá hiệu năng.				

Mã tham chiếu	Nội dung/ Yêu cầu cần đạt		Yêu cầu cần đạt theo hạng			
	Kiến thức	Kỹ năng	4	3	2	1
	- Các yêu cầu vận hành hệ thống CSDL. - Tiến trình rà soát. - Các mục và ghi chú cần được đưa vào trong tài liệu xác định yêu cầu CSDL.	- Đề xuất cách thức bảo đảm hiệu năng. - Chuyển các yêu cầu an toàn thông tin của người sử dụng thành các yêu cầu an toàn thông tin của hệ thống CSDL. - Chuyển các yêu cầu vận hành người sử dụng thành các yêu cầu của hệ thống CSDL. - Mô tả các yêu cầu quan trọng một cách rõ ràng và chính xác. - Lựa chọn phương pháp truyền thông phù hợp với việc rà soát các yêu cầu và thúc đẩy tiến độ đánh giá một cách hiệu quả. - Cân nhắc các ý kiến trái ngược một cách phù hợp.				
DBSS 3	**Mô đun: Phân tích và thiết kế CSDL**			x	x	x
DBSS 3.1	Xây dựng mô hình dữ liệu mức khái niệm					
	- Phương pháp xây dựng mô hình. - Biểu đồ quan hệ thực thể (ERD - Entity Relationship Diagram) và các mô hình CSDL khác. - Quy tắc nghiệp vụ. - Giao diện đồ họa người sử dụng (GUI - Graphic User Interface).	- Phân tích cấu trúc thông tin, phân tích hướng đối tượng (Biểu đồ lớp). - Chuyển các yêu cầu của người sử dụng vào mô hình mức khái niệm. - Xác định thuộc tính thực thể. - Xác nhận sự nhất quán giữa quy trình nghiệp vụ và mô hình dữ liệu. - Điều chỉnh sự khác biệt giữa một số mô hình mức khái niệm. - Nhận biết và giải quyết các yêu cầu mâu thuẫn nhau. - Lập các tài liệu dễ đọc về mô hình dữ liệu mức khái niệm cho người phát triển ứng dụng và người sử dụng.				
DBSS 3.2	Kiểm chứng mô hình dữ liệu mức khái niệm					
	- Mô hình tổ chức. - Quy trình nghiệp vụ. - Cơ sở dữ liệu (CSDL).	- Nắm bắt những mối quan tâm chính của người sử dụng. - Giải thích mô hình dữ liệu cho kỹ sư phát triển ứng dụng và người sử dụng. - Xác nhận sự nhất quán giữa các				

Mã tham chiếu	Nội dung/ Yêu cầu cần đạt		Yêu cầu cần đạt theo hạng			
	Kiến thức	Kỹ năng	4	3	2	1
		mô hình tổ chức và mô hình dữ liệu. - Nhận biết và giải quyết các yêu cầu mâu thuẫn. - Giải thích sự thay đổi của mô hình dữ liệu cho những người quan tâm để được chấp thuận. - Lập tài liệu dễ hiểu về mô hình dữ liệu cho kỹ sư phát triển ứng dụng và người sử dụng.				
DBSS 3.3	Thiết kế mô hình dữ liệu mức logic					
	- CSDL quan hệ, mô hình dữ liệu quan hệ. -Xây dựng bảng dữ liệu trong CSDL quan hệ. - Hiệu suất thực thi CSDL - Hiểu biết về quy tắc chuyển đổi từ biểu đồ ERD sang cấu trúc SQL và NoSQL. - Chuẩn hóa. - Các hạn chế của tính toàn vẹn. - Giao diện đồ họa người sử dụng (GUI).	- Chuyển đổi từ mô hình dữ liệu ERD sang mô hình dữ liệu quan hệ. - Thực hiện chuẩn hóa. - Chỉ ra hạn chế của mô hình dữ liệu ERD. - Phân tích hướng đối tượng (Biểu đồ lớp); Quyết định về các kiểu dữ liệu, các chỉ mục và Quyết định việc dư thừa dữ liệu và thuyết minh lý do.				
DBSS 3.4	Kiểm chứng mô hình dữ liệu mức logic					
	- Mô hình của tổ chức. - Quy trình nghiệp vụ. - Cơ sở dữ liệu.	- Kiểm chứng dữ liệu về độ chính xác và tính phù hợp với mục tiêu của dự án. - Lập tài liệu dễ hiểu về mô hình dữ liệu cho người phát triển ứng dụng.				
DBSS 4	**Mô đun: Xây dựng và kiểm thử CSDL**			x	x	x
DBSS 4.1	Lựa chọn và cài đặt hệ quản trị CSDL					
	- Các phương pháp thu thập thông tin từ nhà cung cấp giải pháp hệ quản trị CSDL (nhà cung cấp). - Các tiêu chí lựa chọn. - Môi trường hiện tại và môi trường cài đặt thời gian thực. - Ứng dụng CSDL. - Thiết kế và triển khai CSDL. - Hiệu năng CSDL. - Tính sẵn sàng.	- Nhận biết, hợp nhất và tóm tắt các yêu cầu khác nhau liên quan đến hệ quản trị CSDL. - Nhận biết sự hài lòng hoặc không hài lòng của các nhóm khách hàng. - So sánh các quan điểm khác nhau. - Đánh giá thông tin từ nhà cung cấp. - Gửi yêu cầu cho nhà cung cấp. - Đàm phán với các nhà cung cấp.				

Mã tham chiếu	Nội dung/ Yêu cầu cần đạt		Yêu cầu cần đạt theo hạng			
	Kiến thức	Kỹ năng	4	3	2	1
	- Các phương pháp cài đặt và đánh giá hệ thống. - Thử nghiệm ứng dụng và dữ liệu. - Tính tích hợp và phát triển mở rộng.	- Thu thập thông tin cài đặt từ các tổ chức khác. - Đánh giá sự phù hợp với mục tiêu của dự án CSDL. - Lựa chọn hệ quản trị CSDL trên cơ sở cân bằng giữa các yếu tố chi phí, chức năng, hiệu suất, tính sẵn sàng. - Nắm bắt các ý kiến đối lập. - Giải thích quy trình và lý do lựa chọn cho những người liên quan.				
DBSS 4.2	Thiết kế CSDL mức vật lý					
DBSS 4.2.1	Xác nhận môi trường vật lý mục tiêu					
	- Môi trường mục tiêu. - Hệ quản trị CSDL mục tiêu.	- Đánh giá hiệu năng mục tiêu.				
DBSS 4.2.2	Phân tích giao dịch					
	- Phương pháp tính toán lượng dữ liệu. - Phương pháp phân tích giao dịch. - Phương pháp phân tích lĩnh vực cốt yếu.	- Phân tích các giao dịch và xác định các yêu cầu sử dụng. - Phân tích các yêu cầu từ góc độ toàn cục.				
DBSS 4.2.3	Các yêu cầu cụ thể về CSDL					
	- Chính sách dữ liệu của tổ chức. - Chính sách sao lưu phục hồi của tổ chức. - Quản lý vận hành hệ thống CSDL. - Hiệu năng truy cập CSDL.	- Chuẩn bị các tài liệu dự phòng cho việc xác định yêu cầu và giải thích lý do. - Phân tích các thông tin yêu cầu và đưa vào yêu cầu tổng hợp chung. - Phân tích và tư duy về việc sử dụng hệ thống ổn định. - Xác định các yêu cầu CSDL phù hợp với mục tiêu. - Khai thác các yêu cầu ban đầu của một CSDL và phát triển các yêu cầu hệ thống chi tiết. - Nhận biết các yêu cầu mâu thuẫn và đưa ra giải pháp.				
DBSS 4.2.4	Thiết kế kiến trúc					
	- Vòng đời dữ liệu (tạo lập, phân phối, xử lý, loại bỏ). - Nhu cầu xử lý dữ liệu tại vị trí của người sử dụng.	- Xác định kiến trúc và chuẩn bị tài liệu. - Phân tích các lưu đồ thông tin và dữ liệu.				

Mã tham chiếu	Nội dung/ Yêu cầu cần đạt		Yêu cầu cần đạt theo hạng			
	Kiến thức	Kỹ năng	4	3	2	1
	- Hệ thống phân tán và CSDL phân tán. - Hệ thống máy chủ, máy trạm. - Ưu điểm và nhược điểm của các CSDL tập trung hoặc phân tán. - Kiến trúc mạng.	- Chuyển các yêu cầu của người sử dụng thành thiết kế kiến trúc. - Hợp nhất và tóm tắt các yêu cầu khác nhau. - Xác định các vấn đề kỹ thuật và đề xuất giải pháp. - Giải thích về quá trình lựa chọn kiến trúc và lý do cho những người liên quan. - Thiết kế dữ liệu phân tán.				
DBSS 4.2.5	Chuyển đổi sang hệ quản trị CSDL mục tiêu					
	- Hệ quản trị CSDL mục tiêu. - Lựa chọn loại dữ liệu. - Nén dữ liệu. - Tính toàn vẹn dữ liệu. - Thiết kế bản ghi vật lý. - Các phương pháp tính toán lượng dữ liệu. - Khóa dữ liệu.	- Tìm hiểu mô hình dữ liệu mức logic. - Xem xét sự ổn định của hệ thống. - Nhận biết hạn chế của hệ quản trị CSDL mục tiêu. - Tính toán không gian lưu trữ cần thiết.				
DBSS 4.2.6	Thiết kế hiệu năng					
	- Hệ quản trị CSDL mục tiêu. - Việc lựa chọn cách truy cập. - Phương pháp điều chỉnh chuẩn hóa. - Việc lựa chọn chỉ số. - Sự phân bổ không gian lưu trữ.	- Xem xét tính ổn định của hệ thống. - Nhận biết hạn chế của hệ quản trị CSDL mục tiêu.				
DBSS 4.2.7	Phân bổ vật lý của dữ liệu					
	- Cấu hình thiết bị lưu trữ.	- Phân tích mật độ truy cập dữ liệu. - Thiết kế vùng dữ liệu phân tán và vùng bản ghi phân tán. - Đánh giá hiệu quả vận hành CSDL.				
DBSS 4.2.8	Thiết kế an toàn thông tin					
	- Đảm bảo an toàn thông tin CSDL. - Kiểm soát truy cập.	- Đánh giá tương quan giữa yêu cầu bảo mật và kiểm soát truy nhập. - Phân quyền thích hợp.				
DBSS 4.3	Triển khai thực hiện					
	- Xác định CSDL thông qua SQL.	- Triển khai hoặc chỉ đạo triển khai xác định CSDL theo hệ quản				

Mã tham chiếu	Nội dung/ Yêu cầu cần đạt		Yêu cầu cần đạt theo hạng			
	Kiến thức	Kỹ năng	4	3	2	1
	- Phương pháp thiết kế dữ liệu. - Việc chuyển đổi dữ liệu	trị CSDL mục tiêu. - Thu thập dữ liệu gốc và chuyển sang định dạng dữ liệu mục tiêu. - Kiểm tra các mô hình dữ liệu, các phần của CSDL.				
DBSS 4.4	Kiểm thử					
	- Phương pháp kiểm tra CSDL - Việc sử dụng các công cụ kiểm tra - Thủ tục kiểm tra khi phát hiện bất thường - Việc kiểm tra so sánh (benchmark) - Lưu trữ và bảo trì tài liệu	- Chuẩn bị dữ liệu phục vụ kiểm thử - Phát hiện bất thường - Phối hợp với đồng nghiệp để đưa ra giải pháp xử lý các tình huống bất thường - Chỉ ra điểm yếu của CSDL và đánh giá ảnh hưởng đối với người sử dụng - Giải thích đối với người liên quan một cách chính xác về những điểm yếu của CSDL có ảnh hưởng đáng kể đối với người sử dụng - Chuẩn bị tài liệu hướng dẫn dễ hiểu, đầy đủ, chính xác				
DBSS 5	**Mô đun: Quản trị, vận hành hệ thống CSDL**		x	x	x	x
DBSS 5.1	Xây dựng kế hoạch vận hành hệ thống CSDL					
	- Phương pháp giám sát. - Công cụ giám sát. - Bảo trì phần cứng. - Cài đặt phần cứng bổ sung. - Phục hồi sao lưu. - Giám sát hệ thống. - Đảm bảo hiệu năng. - Toàn vẹn dữ liệu. - An toàn thông tin và dữ liệu.	- Xây dựng chính sách quản lý hệ thống trên cơ sở ngân sách có được. - Giải thích chính sách quản lý vận hành cho người sử dụng. - Nhận thức được tầm quan trọng của việc giám sát. - Liệt kê các bất thường. - Nghiên cứu việc vận hành hệ thống ổn định. - Đề xuất các biện pháp đối phó với bất thường. - Lập kế hoạch cài đặt bổ sung.				
DBSS 5.2	Vận hành và bảo trì hệ thống CSDL					
	- Phương pháp thu thập dữ liệu giám sát. - Sử dụng các công cụ giám sát. - Phương pháp phân tích dữ liệu giám sát. - Hệ điều hành.	- Phân tích dữ liệu giám sát. - Mô tả các phân tích một cách chi tiết và chính xác trong tài liệu. - Thực hiện các biện pháp thích hợp khi phát hiện các điều kiện bất thường.				

Mã tham chiếu	Nội dung/ Yêu cầu cần đạt		Yêu cầu cần đạt theo hạng			
	Kiến thức	Kỹ năng	4	3	2	1
	- Những tác động khi cập nhật phần mềm. - Các ứng dụng CSDL. - Xây dựng chuẩn.	- Xác định thời điểm thích hợp để cập nhật phần mềm. - Thiết lập quy tắc sử dụng ứng dụng mới. - Giám sát tình trạng tuân thủ chuẩn và thúc đẩy sự cải tiến. - Chuẩn bị các tài liệu về chuẩn. - Giải thích sự sai lệch so với chuẩn có thể làm giảm hiệu năng và khả năng bảo trì. - Xác định các chuẩn không còn thích ứng với tình trạng thực tế và cần loại bỏ.				
DBSS 5.3	Quản trị hệ thống CSDL					
DBSS 5.3.1	Bảo tồn tính toàn vẹn					
	- Mô hình dữ liệu.	- Nhận biết, phát hiện những khiếm khuyết về tính toàn vẹn. - Thực hiện các giải pháp khắc phục những khiếm khuyết về tính toàn vẹn.				
DBSS 5.3.2	Bảo tồn cấu trúc vật lý của dữ liệu					
	- Ứng dụng CSDL.	- Phân tích báo cáo truy vấn. - Phân tích các yêu cầu của người sử dụng, thực hiện giải pháp và đánh giá tác động.				
DBSS 5.3.3	Quản lý phục hồi sao lưu					
	- Môi trường hệ thống. - Sao lưu phục hồi.	- Giải thích tình trạng sao lưu cho người sử dụng.				
DBSS 5.3.4	Quản lý các yêu cầu về tài nguyên vật lý					
	- Giới hạn của các tài nguyên vật lý. - Khả năng của tài nguyên vật lý. - Phương pháp đo lường trạng thái sử dụng tài nguyên. - Các ứng dụng CSDL.	- Đo lường việc sử dụng tài nguyên. - Nắm bắt xu hướng sử dụng tài nguyên một cách chính xác. - Dự báo việc mở rộng sử dụng tài nguyên. - Đánh giá sự cần thiết phải nâng cấp tài nguyên. - Xác định việc sử dụng bất thường các tài nguyên.				
DBSS 5.3.5	Các biện pháp ứng phó với việc kiểm tra CSDL					
	- Việc kiểm tra (audit) hệ thống. - Thủ tục kiểm tra CSDL.	- Giải thích chính xác tình trạng quản trị vận hành hệ thống với nhân viên kiểm tra hệ thống.				

Mã tham chiếu	Nội dung/ Yêu cầu cần đạt		Yêu cầu cần đạt theo hạng			
	Kiến thức	Kỹ năng	4	3	2	1
		- Nắm bắt các tiêu chí kiểm tra và các biện pháp ứng phó với việc kiểm tra.				
DBSS 5.4	Điều chỉnh hiệu năng CSDL					
	- Thiết kế hiệu năng. - Thiết kế bảng. - Thiết kế chỉ số. - Phân bổ vật lý. - Truy cập thiết bị lưu trữ. - Cải tiến hiệu năng.	- Xác định nguyên nhân giảm hiệu năng. - Vận dụng các bài học cải tiến như một cách điều chỉnh hiệu năng. - Đảm bảo chắc chắn không có tác động tiêu cực phát sinh do việc thực hiện điều chỉnh hiệu năng. - Đánh giá sự cần thiết phải tăng cường thiết bị.				
DBSS 5.5	Hỗ trợ người sử dụng					
DBSS 5.5.1	Cung cấp môi trường phát triển CSDL và hỗ trợ sử dụng					
	- Hệ quản trị CSDL. - Hệ điều hành. - Các ứng dụng CSDL. - Phát triển CSDL.	- Thiết lập hoặc sửa đổi các chuẩn phát triển CSDL và các ứng dụng CSDL. - Tạo sự thuận lợi cho người phát triển ứng dụng CSDL.				
DBSS 5.5.2	Cung cấp môi trường sử dụng CSDL					
	- Các ứng dụng của người sử dụng. - Việc sử dụng phần mềm của người sử dụng.	- Giảm thiểu tác động đối với người sử dụng do sự thay đổi của mô hình dữ liệu.				
DBSS 5.5.3	Xây dựng và thực hiện kế hoạch đào tạo người sử dụng					
	- Cách thức thúc đẩy tiến trình đào tạo người sử dụng.	- Xây dựng kế hoạch đào tạo và hỗ trợ theo khả năng sử dụng phần mềm của người sử dụng. - Đánh giá kỹ năng của người sử dụng và phản ánh chi tiết các kết quả đào tạo. - Phân tích quá trình đào tạo người sử dụng. - Phân tích nhu cầu của người sử dụng về đào tạo và các biện pháp đáp ứng.				
DBSS 5.5.4	Khảo sát các yêu cầu bổ sung của người sử dụng					
	- Thu thập thông tin về yêu cầu của người sử dụng. - Phân tích yêu cầu.	- Chuyển các yêu cầu của người sử dụng thành các yêu cầu về công nghệ của hệ thống. - Giải thích phù hợp các yêu cầu				

Mã tham chiếu	Nội dung/ Yêu cầu cần đạt		Yêu cầu cần đạt theo hạng			
	Kiến thức	Kỹ năng	4	3	2	1
		không đúng của người sử dụng.				

PHỤ LỤC SỐ 03
YÊU CẦU VỀ KIẾN THỨC, KỸ NĂNG CHUYÊN SÂU CỦA CHUẨN KỸ NĂNG HỆ THỐNG MẠNG

(Ban hành kèm theo Thông tư số 11/2015/TT-BTTTT ngày 5/5/2015 của Bộ trưởng Bộ Thông tin và Truyền thông)

Mã tham chiếu	Nội dung/ Yêu cầu cần đạt		Yêu cầu cần đạt theo hạng			
	Kiến thức	Kỹ năng	4	3	2	1
NWSS1	**Mô đun: Xác định yêu cầu về hệ thống mạng**				**x**	**x**
NWSS 1.1	Phân tích yêu cầu sử dụng mạng					
	-Phương pháp, quy trình và thực hiện thu thập thông tin. - Xác định mục tiêu và phạm vi khảo sát. - Kiến trúc mạng, topo mạng, phần cứng và phần mềm. - Công nghệ kết nối mạng và môi trường vận hành mạng. - Thiết kế mạng. - Cấu hình hệ thống. - Cấu hình phần mềm ứng dụng và phần mềm trung gian (middleware). - Các hạn chế công nghệ, các chuẩn phần cứng, phần mềm và quy trình xử lý. - Các kỹ thuật phân tích rủi ro.	- Xác định các nguồn thông tin chính về nhu cầu của người sử dụng. - Xác định lượng thông tin cần thu thập. - Phân tích phản hồi của các cá nhân và nhóm. - Lựa chọn, thu thập dữ liệu liên quan đến các nhiệm vụ và xác định nhu cầu về dữ liệu. - Sắp xếp và tóm lược thông tin về yêu cầu. - Phân tích và xác định sự phụ thuộc lẫn nhau của thông tin. - Xây dựng tài liệu tham khảo chi tiết về các hạn chế của công nghệ. - Tổ chức các cuộc thảo luận tự do và xác nhận các câu hỏi. - Làm việc nhóm.				
NWSS 1.2	Phân tích hệ thống mạng hiện có					
	- Phương pháp thu thập thông tin. - Đo lường lưu lượng mạng. - Các công cụ phân tích lưu lượng. - Cấu hình hệ thống. - Cấu hình mạng. - Cấu hình phần mềm ứng dụng, phần mềm trung gian.	- Đo lường và đánh giá lưu lượng mạng. - Xác định các khả năng nghẽn mạng trên cơ sở cấu hình hệ thống. - Phân tích hệ thống.				
NWSS 1.3	Xác định phạm vi công việc					
	- Kiến trúc mạng, topo mạng, phần cứng và phần mềm. - Công nghệ kết nối mạng và	- Xây dựng tài liệu chi tiết về phạm vi công việc. - Sắp xếp các yêu cầu để đáp ứng				

Mã tham chiếu	Nội dung/ Yêu cầu cần đạt		Yêu cầu cần đạt theo hạng			
	Kiến thức	**Kỹ năng**	**4**	**3**	**2**	**1**
	môi trường vận hành. - Tài nguyên sẵn có và thời gian hoàn thành dự án. - Khối lượng công việc. - Các hạn chế công nghệ.	mục tiêu. - Dự đoán kết quả phát triển theo kinh nghiệm và kiến thức có được. - Lập kế hoạch trên cơ sở các khả năng về nguồn lực và hạn chế. - Trình bày trực quan các nhiệm vụ cần thực hiện theo cách tuần tự hoặc song song. - Đàm phán về các tiêu chí cần đạt được. - Xem xét tổng thể nhiều vấn đề.				
NWSS 1.4	Xác định các yêu cầu về hệ thống mạng					
	- Hệ thống và khả năng tích hợp của hệ thống. - Công nghệ kết nối mạng và môi trường vận hành. - Kiến trúc mạng, topo mạng, phần cứng và phần mềm. - Các yêu cầu về hiệu năng. - An toàn thông tin mạng. - Vòng đời của hệ thống. - Độ tin cậy của mạng. - Các yêu cầu vận hành mạng. - Cách thức thực hiện rà soát.	- Phản ánh các yêu cầu xử lý thông tin của tổ chức dưới dạng các yêu cầu đối với hệ thống. - Xác định mong muốn của người sử dụng. - Nhận biết mâu thuẫn giữa các yêu cầu và đưa ra cách khắc phục. - Phân tích tính chính xác và nhất quán của thông tin. - Giải quyết các vấn đề về công nghệ. - Đánh giá cấu hình của hệ thống. - Lập tài liệu tham khảo chi tiết bổ trợ cho các yêu cầu. - Quan sát các đối tượng từ nhiều khía cạnh khác nhau.				
NWSS 2	**Mô đun: Thiết kế hệ thống mạng**				**x**	**x**
NWSS 2.1	Khảo sát, đánh giá công nghệ và sản phẩm sẽ áp dụng					
	- Phương pháp thu thập thông tin. - Kiến trúc mạng, topo mạng, phần cứng và phần mềm. - Các hạn chế công nghệ, các chuẩn phần cứng, phần mềm và quy trình xử lý.	- Phân tích và xác định sự phụ thuộc lẫn nhau của thông tin. - Giải thích thông tin công nghệ bằng các công cụ thích hợp. - Lập tài liệu tham khảo chi tiết về các hạn chế của công nghệ.				
NWSS 2.2	Thiết kế hệ thống mạng					
NWSS 2.2.1	Xác định kiến trúc mạng					
	- Cấu hình hệ thống của ứng dụng. - Dịch vụ lớp cao trong mô hình OSI.	- Phân biệt giữa các yêu cầu thực tế và công nghệ mong muốn. - Dự đoán các kết quả dựa trên những trải nghiệm trong quá khứ				

Mã tham chiếu	Nội dung/ Yêu cầu cần đạt		Yêu cầu cần đạt theo hạng			
	Kiến thức	Kỹ năng	4	3	2	1
	- Các chuẩn và quy trình công nghệ kết nối mạng. - Các công cụ và phương pháp thiết kế kiến trúc mạng. - Kiến trúc mạng, topo mạng, phần cứng và phần mềm. - Sơ đồ thông tin. - Loại thông tin và lưu lượng. - Thông lượng (throughput). - Thống kê về ước lượng tải lưu lượng và thông lượng.	và kiến thức hiện có. - Phân tích xu thế bằng phương pháp dự báo. - Phân tích thông tin công nghệ và giải thích một cách rõ ràng và ngắn gọn.				
NWSS 2.2.2	Biện pháp an toàn thông tin					
	- An toàn hệ thống và những lỗ hổng bảo mật tiềm tàng. - An toàn mạng. - Cách thức bảo vệ thông tin. - Văn bản quy phạm pháp luật về an toàn thông tin	- Nhận biết và triển khai chính sách an toàn thông tin. - Đánh giá, sửa đổi các tiêu chí về an toàn thông tin. - Phát hiện các vấn đề về an toàn thông tin ở khía cạnh đạo đức. - Xác định các loại rủi ro.				
NWSS 2.2.3	Biện pháp tin cậy					
	- Độ tin cậy. - Hiệu quả kinh tế (cân bằng giữa chi phí lắp đặt và chi phí vận hành, bảo trì). - Các dịch vụ truyền thông tin.	- Nhận biết mức độ yêu cầu đối với các biện pháp tin cậy của ứng dụng. - Cân bằng các biện pháp tin cậy và các chi phí cần thiết.				
NWSS 2.2.4	Kịch bản thiết kế					
	- Các tiêu chuẩn và quy trình xử lý kết nối mạng. - Cấu hình hệ thống của ứng dụng. - Kiến trúc mạng, topo mạng, phần cứng và phần mềm. - Công nghệ mạng và cách cài đặt các chức năng của thiết bị. - Tính tích hợp và phát triển mở rộng của giải pháp.	- Tái sử dụng tối ưu phần cứng hiện có. - Xây dựng các sơ đồ khối và sử dụng các công cụ vẽ biểu đồ. - Dự đoán những kết quả dựa trên kiến thức sẵn có. - Trình bày ý tưởng, thông tin phức tạp. - Đánh giá các kế hoạch khác nhau và lựa chọn một kế hoạch hợp lư. - Đưa các chuẩn và thủ tục vào các tài liệu kỹ thuật.				
NWSS 2.3	Lập kế hoạch vận hành cho hệ thống mạng mới					
	- Hoạt động nghiệp vụ. - Các bên liên quan và các nhóm làm việc. - Các thủ tục chuyển đổi.	- Trình bày vấn đề, yêu cầu và đặt câu hỏi và tổ chức sắp xếp các câu hỏi. - Xác định các nhu cầu thông tin.				

Mã tham chiếu	Nội dung/ Yêu cầu cần đạt		Yêu cầu cần đạt theo hạng			
	Kiến thức	**Kỹ năng**	**4**	**3**	**2**	**1**
	- Các vấn đề tổ chức liên quan đến an toàn thông tin.	- Thúc đẩy hợp tác. - Phân tích và tổng hợp thông tin. - Sử dụng phần mềm quản lý dự án. - Duy trì các quy trình tổ chức dựa trên các quy tắc của tổ chức. - Tìm hiểu ứng dụng của người sử dụng và liên kết nhu cầu của họ với cấu hình của ứng dụng. - Phân tích trực quan mối quan hệ giữa các bộ phận và tổng thể cũng như các quy trình và thủ tục.				
NWSS 2.4	Lập kế hoạch thực hiện					
	- Phương pháp tích hợp và công cụ phân tích lưu lượng. - Cách thức thực hiện kế hoạch và ảnh hưởng đối với người sử dụng. - Mạng và môi trường vận hành.	- Thu thập và phân tích thông tin. - Giải thích rõ ràng các thông tin về công nghệ. - Giải thích và tổng hợp kết quả. - Phân tích thông tin, tình huống và lập kế hoạch trong giới hạn nghiệp vụ và tài chính. - Lập kế hoạch hoạt động, phối hợp hoạt động và thực hiện kế hoạch. - Sử dụng các công cụ quản lý dự án và phần mềm lập lịch. - Dự toán chi phí thiết kế, xây dựng và chi phí vận hành, bảo trì hệ thống.				
NWSS 2.5	Rà soát thiết kế					
	- Các thủ tục rà soát thiết kế. - Kiến trúc mạng, topo mạng, phần cứng và phần mềm. - Mạng và môi trường vận hành.	- Truyền đạt thông tin về công nghệ cho những người sử dụng khác nhau. - Giải thích rõ ràng các thông tin về công nghệ. - Lắng nghe ý kiến phê bình mang tính xây dựng. - Giải thích rõ ràng thông tin về công nghệ và sử dụng các công cụ thích hợp để giải thích.				
NWSS 3	**Mô đun: Xây dựng và thử nghiệm hệ thống mạng**		**x**	**x**	**x**	**x**
NWSS 3.1	Thực hiện các bước chuẩn bị					
	- Cấu hình hệ thống. - Cài đặt phần mềm và các thủ	- Phân tích thông tin và tình huống.				

Mã tham chiếu	Nội dung/ Yêu cầu cần đạt		Yêu cầu cần đạt theo hạng			
	Kiến thức	Kỹ năng	4	3	2	1
	tục để thiết đặt cấu hình. - Các bên liên quan và nhóm làm việc.	- Xem xét rủi ro. - Chuẩn bị các kế hoạch khác nhau. - Xây dựng kế hoạch hoạt động. - Tuân thủ các thủ tục thích hợp. - Lập tài liệu chi tiết về luồng quy trình nghiệp vụ. - Đàm phán và phối hợp cho đến khi các bên liên quan đồng ý để cài đặt.				
NWSS 3.2	Cài đặt mạng					
	- Cài đặt phần mềm và các thủ tục để cấu hình. - Các vấn đề chuyển đổi dữ liệu và các thủ tục thực hiện. - Các vấn đề về tương thích và các thủ tục thực hiện. - Cấu hình phần cứng. - Kiến trúc mạng, topo mạng, phần cứng và phần mềm.	- Xây dựng ứng dụng mới. - Trình bày các thông tin về công việc cài đặt cho người sử dụng. - Xem xét các ý kiến (lời nói hoặc văn bản) và có phản hồi thích hợp. - Áp dụng chiến lược cải tiến liên tục và các công cụ hỗ trợ. - Giải quyết kịp thời các mâu thuẫn. - Tổ chức nhiều lịch trình và quản lý các mốc quan trọng, đưa ra các điều chỉnh cần thiết. - Minh họa tác động về hiệu suất và thực hiện các điều chỉnh cần thiết.				
NWSS 3.3	Chuẩn bị thử nghiệm					
	- Các công cụ và thủ tục thử nghiệm. - Các yêu cầu nghiệp vụ. - Các ứng dụng. - Môi trường mạng. - Các ảnh hưởng của lỗi đến hiệu năng hệ thống. - Ngân sách cần thiết và cơ cấu tổ chức. - Kiến trúc mạng, topo mạng, phần cứng và phần mềm.	- Thực hiện việc phân tích hệ thống. - Truyền đạt và hiểu thông tin. - Phân tích và xây dựng cấu trúc hệ thống. - Xác định các thiết bị thử nghiệm. - Liên kết các lỗi với chức năng của hệ thống. - Phân tích nguyên nhân/ lý do của các vấn đề và đề xuất kế hoạch hành động. - Phân tích dữ liệu. - Đánh giá mức độ phù hợp của các tình huống nghiệp vụ với cấu trúc hệ thống. - Đàm phán để cung cấp các				

Mã tham chiếu	Nội dung/ Yêu cầu cần đạt		Yêu cầu cần đạt theo hạng			
	Kiến thức	Kỹ năng	4	3	2	1
		nguồn lực cần thiết. - Nhận biết các điểm mạnh và hạn chế của hệ thống.				
NWSS 3.4	Thử nghiệm mạng					
	- Phương pháp thực hiện thử nghiệm và các thủ tục. - Kiến trúc mạng, topo mạng, phần cứng và phần mềm.	- Sử dụng các công cụ lập kế hoạch. - Giải quyết vấn đề về quy trình và thủ tục trong phạm vi trách nhiệm của mình. - Phân tích phản biện các chi tiết. - Ghi lại các kết quả thử nghiệm. - Xem xét cách thức phù hợp để thúc đẩy quy trình. - Kiểm soát các mốc quan trọng. - Khuyến khích và hỗ trợ các thành viên của nhóm và phân công trách nhiệm để đạt mục tiêu của nhóm.				
NWSS 3.5	Phân tích và đánh giá kết quả thử nghiệm					
	- Sản phẩm và mối tương quan trong môi trường thử nghiệm. - Quy trình cải tiến liên tục để thực hiện thử nghiệm. - Các thủ tục báo cáo trong tổ chức.	- Áp dụng các quy tắc/nguyên tắc đối với quy trình/dữ liệu và lập luận logic để rút ra kết luận. - Giải thích về các ý tưởng/thông tin phức tạp. - Xem xét phương pháp giải quyết vấn đề một cách sáng tạo và xây dựng kế hoạch/phương pháp tiếp cận mới. - Nắm bắt và chuyển các kết quả thử nghiệm vào trong các tình huống thực.				
NWSS 4	**Mô đun: Vận hành và bảo trì hệ thống mạng**		**x**	**x**	**x**	**x**
NWSS 4.1	Thực hiện các bước chuẩn bị cho người sử dụng					
	- Chính sách và thủ tục của tổ chức. - Việc mở rộng các thủ tục. - Lập và lưu trữ tài liệu. - Các công cụ an toàn thông tin. - Hệ điều hành và hệ thống mạng. - Thiết lập mạng cho người sử dụng.	- Áp dụng các quy tắc, thủ tục cho tài khoản và lập tài liệu. - Mô tả nội dung các thủ tục bảo trì. - Tuân thủ các quy tắc, chính sách và thủ tục. - Xác định và giải quyết các vấn đề. - Tiếp nhận các câu hỏi và xác định nội dung câu hỏi.				
NWSS 4.2	Xây dựng chính sách bảo trì, cập nhật và nâng cấp					

Mã tham chiếu	Nội dung/ Yêu cầu cần đạt		Yêu cầu cần đạt theo hạng			
	Kiến thức	Kỹ năng	4	3	2	1
	- Các hệ thống nghiệp vụ. - Vòng đời của hệ thống mạng. - Kiến trúc mạng, topo mạng, phần cứng và phần mềm. - Sự phụ thuộc giữa hệ điều hành và hệ thống. - Các thủ tục sao lưu.	- Xác định nhu cầu và mong muốn của người sử dụng. - Dự đoán kết quả dựa trên kiến thức đã có. - Đề xuất và thực hiện kế hoạch hành động. - Giải thích về các ý tưởng và thông tin phức tạp. - Đánh giá cấu hình và sự ổn định của hệ thống. - Thu thập thường xuyên thông tin về sản phẩm mới.				
NWSS 4.3	Lập kế hoạch bảo trì					
	- Các công cụ và thủ tục bảo trì. - Các thủ tục vận hành hệ thống mạng của tổ chức.	- Đánh giá tác động của các lỗi kỹ thuật. - Lập tài liệu hỗ trợ một cách chi tiết và rõ ràng. - Đàm phán hướng tới thỏa thuận. - Dự đoán các kết quả về mặt công nghệ. - Nắm bắt và truyền đạt thông tin cho các bên có liên quan một cách thuyết phục và đáp ứng mục tiêu.				
NWSS 4.4	Thực hiện bảo trì, cập nhật và nâng cấp					
	- Các thủ tục thực hiện cập nhật. - Lý do cập nhật. - Các vấn đề chuyển đổi dữ liệu và các thủ tục cũng như các vấn đề tương thích và thủ tục giải quyết. - Kiến trúc mạng, topo mạng, phần cứng và phần mềm. - Thủ tục bảo trì. - Các thủ tục và tiêu chuẩn lập tài liệu bảo trì.	- Thực hiện việc cải tiến, sửa đổi phù hợp với sự phát triển của công nghệ. - Đánh giá cấu hình, tính ổn định của hệ thống. - Lập kế hoạch quy trình thực hiện. - Tuân thủ các thủ tục phù hợp. - Tìm hiểu việc vận hành, đáp ứng của hệ thống. - Tìm hiểu và đánh giá các dữ liệu nhận được. - Trình bày thông tin một cách rõ ràng và chính xác.				
NWSS 4.5	Sao lưu và phục hồi dữ liệu					
	- Các thủ tục sao lưu và phục hồi dữ liệu. - Kiến trúc mạng, topo mạng,	- Nhận biết các vấn đề trong hệ thống và đánh giá tầm quan trọng của chúng.				

Mã tham chiếu	Nội dung/ Yêu cầu cần đạt		Yêu cầu cần đạt theo hạng			
	Kiến thức	Kỹ năng	4	3	2	1
	phần cứng và phần mềm. - Các phương tiện sao lưu. - Các quy định về lưu trữ điện tử.	- Thực hiện các thủ tục. - Lập tài liệu tài liệu hỗ trợ chi tiết trên cơ sở các thông tin và các hoạt động. - Đánh giá tác động của các hành động.				
NWSS 4.6	Quản lý cấu hình hệ thống mạng					
	- Thực hiện đăng ký (registry) trong cơ sở dữ liệu và truy nhập cơ sở dữ liệu. - Các thủ tục của tổ chức trong việc mua sắm và kiểm soát đầu tư.	- Sử dụng các công cụ kiểm soát thành phần mạng. - Sử dụng cơ sở dữ liệu đăng ký. - Lập các tài liệu hỗ trợ chi tiết. - Thực hiện việc giám sát về sử dụng an toàn và hiệu quả tài nguyên. - Phối hợp với người sử dụng liên quan đến việc phân bổ bộ nhớ. - Thực hiện giám sát cấu trúc mạng và việc sử dụng hiệu quả các tài nguyên được đầu tư.				
NWSS 5	**Mô đun: Quản lý hệ thống mạng**		x	x	x	x
NWSS 5.1	Thực hiện công việc giám sát mạng					
	- Phương pháp thu thập dữ liệu giám sát. - Cách sử dụng các công cụ giám sát. - Hệ điều hành. - Các ứng dụng. - Kiến trúc mạng, topo mạng, phần cứng và phần mềm. - Mạng LAN, WAN và các mô hình mạng khác. - Chính sách và thủ tục an toàn thông tin của tổ chức. - Việc lập tài liệu, lưu trữ và các công cụ an toàn thông tin.	- Phân tích dữ liệu giám sát. - Lập các tài liệu có nội dung phân tích một cách chi tiết. - Nắm bắt các xu hướng về hiệu năng và chẩn đoán sai lệch về hiệu năng. - Sử dụng phần mềm quản lý dự án. - Phân tích hoạt động của hệ thống và tác động, hiệu quả của hệ thống.				
NWSS 5.2	Phân tích sự cố và phục hồi					
	- Phương pháp phân tích dữ liệu giám sát. - Hệ điều hành. - Các ứng dụng. - Kiến trúc mạng, topo mạng, phần cứng và phần mềm. - Mạng LAN, WAN và các mô	- Thực hiện các biện pháp thích hợp khi có sự cố bất thường. - Giải thích và đánh giá số liệu. - Thực hiện xử lý sự cố khi có trục trặc và ngừng hệ thống. - Nắm bắt các xu hướng về hiệu năng và chẩn đoán sai lệch về hiệu				

Mã tham chiếu	Nội dung/ Yêu cầu cần đạt		Yêu cầu cần đạt theo hạng			
	Kiến thức	Kỹ năng	4	3	2	1
	hình mạng khác. - Các cấu phần và thiết bị điều khiển của mạng. - Các thủ tục khắc phục sự cố.	năng. - Viết báo cáo theo dõi sự cố và đề xuất xử lý lỗi.				
NWSS 5.3	Phân tích hiệu năng hệ thống					
	- Kiến trúc mạng, topo mạng, phần cứng và phần mềm. - Trạng thái lưu lượng mạng. - Phản hồi của hệ thống. - Vòng đời của hệ thống.	- Sử dụng các công cụ đo lường và giám sát mạng. - Phân tích hệ thống. - Sử dụng các công cụ kiểm tra. - Phân tích và đánh giá độ chính xác dữ liệu. - Chẩn đoán giới hạn về hiệu năng. - Nắm bắt xu hướng hiệu năng và chẩn đoán sai lệch về hiệu năng.				
NWSS 5.4	Phân tích và đối phó với các vi phạm về an toàn thông tin.					
	- Kiến trúc mạng, topo mạng, phần cứng và phần mềm. - Các thủ tục giám sát. - Các công cụ phát hiện xâm nhập trái phép. - Các biện pháp đối phó với hành vi vi phạm an toàn thông tin. - Lỗ hổng an toàn thông tin và bản vá lỗi. - Virus máy tính.	- Đối phó thích hợp tại thời điểm vi phạm. - Sử dụng các công cụ giám sát mạng và công cụ phát hiện xâm nhập trái phép. - Sử dụng các công cụ phòng ngừa. - Thu thập thông tin một cách thường xuyên.				
NWSS 6	**Mô đun: Đánh giá hệ thống mạng**			**x**	**x**	**x**
NWSS 6.1	Đánh giá hệ thống mạng					
	- Thủ tục đánh giá, thủ tục giám sát, thủ tục báo cáo và chính sách của hệ thống mạng trong tổ chức. - Các nguồn lực của tổ chức và các hạn chế của nguồn lực - Quy trình, thủ tục giám sát trên hệ thống. - Các chuẩn lập tài liệu và các thủ tục để phổ biến trong nội bộ tổ chức	- Phân tích và tích hợp thông tin. - Sử dụng các công cụ lập mô hình và mô phỏng. - Đánh giá, điều chỉnh kế hoạch hoạt động. - Xác định các điểm cần cải tiến. - Báo cáo công tác đánh giá hệ thống một cách dễ hiểu.				
NWSS 6.2	Đưa ra đề xuất cải tiến hệ thống mạng					
	- Vòng đời của hệ thống mạng. - Dự báo lưu lượng mạng và yêu cầu của hệ thống mạng	- Đề xuất các sửa đổi và cải tiến hệ thống và phân tích các mục tiêu, ràng buộc.				

Mã tham chiếu	Nội dung/ Yêu cầu cần đạt		Yêu cầu cần đạt theo hạng			
	Kiến thức	**Kỹ năng**	**4**	**3**	**2**	**1**
	- Phương pháp thu thập thông tin. - Hạn chế công nghệ và các chuẩn phần cứng, phần mềm và quy trình xử lý.	- Thu thập thông tin thường xuyên về các sản phẩm mới. - Nắm bắt xu hướng cấu hình hệ thống mạng của các tổ chức khác.				
NWSS 7	**Mô đun: Tư vấn phát triển hệ thống mạng**				x	x
NWSS 7.1	Tư vấn về lập kế hoạch và phân tích hệ thống mạng					
	- Vòng đời của hệ thống mạng. - Đánh giá hệ thống mạng. - Dự báo hướng phát triển hệ thống mạng - Quản lý hệ thống mạng	- Nắm bắt xu hướng về cấu hình của hệ thống mạng trong các tổ chức khác. - Tổng hợp những điểm chính trong các cuộc thảo luận tự do. - Làm việc nhóm. - Thuyết trình.				
NWSS 7.2	Tư vấn về thiết kế và xây dựng hệ thống mạng					
	- Thiết kế và xây dựng hệ thống mạng.	- Nắm bắt xu hướng về cấu hình của hệ thống mạng trong các tổ chức khác. - Tổng hợp những điểm chính trong các cuộc thảo luận tự do. - Làm việc nhóm. - Thuyết trình.				
NWSS 7.3	Tư vấn về vận hành và bảo trì hệ thống mạng					
	- Việc vận hành và quản lý hệ thống mạng.	- Nắm bắt xu hướng về cấu hình của hệ thống mạng trong các tổ chức khác. - Tổng hợp những điểm chính trong các cuộc thảo luận tự do. - Làm việc nhóm. - Thuyết trình.				

PHỤ LỤC SỐ 04
YÊU CẦU VỀ KIẾN THỨC, KỸ NĂNG CHUYÊN SÂU CỦA CHUẨN KỸ NĂNG QUẢN LÝ HỆ THỐNG CNTT

(Ban hành kèm theo Thông tư số 11/2015/TT-BTTTT ngày 5/5/2015 của Bộ trưởng Bộ Thông tin và Truyền thông)

Mã tham chiếu	Nội dung/ Yêu cầu cần đạt		Yêu cầu cần đạt theo hạng			
	Kiến thức	Kỹ năng	4	3	2	1
SMSS 1	**Mô đun: Lập kế hoạch quản lý hệ thống**				x	x
SMSS 1.1	Xác định các yêu cầu quản lý hệ thống					
	- Nội dung và các điều khoản liên quan đến công việc của người sử dụng. - Việc thu thập thông tin. - Các phương pháp phân tích vấn đề. - Các xu hướng hiện tại và tương lai của loại hình nghiệp vụ, ngành nghề, lĩnh vực hoạt động của tổ chức. - Các xu hướng hiện tại và tương lai của CNTT. - Việc vận hành quản lý tổng thể hệ thống. - Quản lý con người.	- Tìm hiểu về chiến lược tin học hóa. - Xác định nguồn thông tin chính về nhu cầu người sử dụng. - Thực hiện các phương pháp và thủ tục thu thập thông tin. - Phân tích phản hồi từ các cá nhân và các nhóm. - Áp dụng phương pháp phân tích công việc để đề xuất cải tiến và cải cách. - Áp dụng phương pháp phân tích vấn đề để giải quyết các vấn đề về quản lý hệ thống. - Lập tài liệu về các kết quả phân tích, kế hoạch cải cách và giải thích cho người sử dụng.				
SMSS 1.2	Xác định các dịch vụ quản lý hệ thống					
	- Công việc của người sử dụng. - Việc sử dụng hệ thống. - Việc quản lý hệ thống - Các rủi ro trong quản lý vận hành hệ thống. - Thực trạng của tổ chức và công nghệ hiện tại. - Phương pháp định lượng nội dung của các dịch vụ.	- Lập tài liệu cho người sử dụng về phạm vi của các dịch vụ. - Đàm phán với người sử dụng về nội dung dịch vụ, các mức dịch vụ và phạm vi trách nhiệm. - Xác định phạm vi và mức dịch vụ phù hợp với ngân sách hiện có. - Xác định các hạn chế về phạm vi và mức độ của các dịch vụ được cung cấp.				
SMSS 1.3	Tính toán chi phí/ lợi ích của các dịch vụ					
	- Kế toán. - Phương pháp hoạch toán chi	- Phân tích các yếu tố hình thành dịch vụ.				

Mã tham chiếu	Nội dung/ Yêu cầu cần đạt		Yêu cầu cần đạt theo hạng			
	Kiến thức	Kỹ năng	4	3	2	1
	phí. - Các yếu tố để tạo/ thay đổi chi phí cho quản lý hệ thống. - Chi phí mua sắm cho tổ chức và các chi phí khác.	- Ước tính số tiền đầu tư vào nguồn lực và chi phí vận hành. - Giải thích chi phí/ lợi ích cho người sử dụng, điều chỉnh (nếu cần thiết) để được chấp thuận.				
SMSS 1.4	Xây dựng quy tắc vận hành					
	- Các công việc quản lý tổng thể hệ thống. - Việc chuẩn hóa và các thủ tục. - Việc sử dụng nguồn lực. - Quản lý thay đổi.	- Cung cấp biểu mẫu thủ tục và tiêu chuẩn hóa các hoạt động hàng ngày. - Xây dựng tài liệu về các quy tắc một cách hoàn chỉnh, chính xác và rõ ràng. - Phát hiện sự khác nhau giữa quy tắc và tình hình thực tế, quyết định về các biện pháp cải tiến. - Giải thích quy tắc để được chấp thuận. - Nắm bắt ý kiến phản biện.				
SMSS 1.5	Xây dựng kế hoạch quản lý hệ thống					
	- Công việc quản lý tổng thể hệ thống. - Việc soạn thảo kế hoạch. - Việc vận hành hệ thống. - Việc bảo trì hệ thống.	- Soạn thảo các kế hoạch ngắn hạn và dài hạn. - Giải thích rõ kế hoạch cho người sử dụng. - Xem xét quản lý hoạt động hệ thống theo quan điểm tổng thể.				
SMSS 2	**Mô đun: Quản lý hệ thống**			x	x	x
SMSS 2.1	Vận hành hệ thống					
	- Việc lập lịch. - Vận hành hệ thống. - Xây dựng tài liệu hướng dẫn sử dụng. - Dữ liệu đánh giá mức độ dịch vụ và cách thức thu thập dữ liệu. - Việc phân tích và đánh giá dữ liệu thu thập được.	- Tạo sự đồng thuận của người sử dụng về sự hợp lý của lịch vận hành. - Xem xét thứ tự công việc và sắp xếp công việc một cách hiệu quả. - Xem xét mức độ khó khăn trong công việc, trình độ kỹ năng của nhân viên phụ trách và ước lượng thời gian vận hành. - Báo cáo cho lãnh đạo về kết quả phân tích, đánh giá tình hình hiện tại và các vấn đề hoạt động của hệ thống.				
SMSS 2.2	Quản lý người sử dụng					

Mã tham chiếu	Nội dung/ Yêu cầu cần đạt		Yêu cầu cần đạt theo hạng			
	Kiến thức	Kỹ năng	4	3	2	1
	- Chính sách và mục đích của việc quản lý người sử dụng. - Quản lý việc đăng ký. - Quản lý an toàn thông tin và tính riêng tư.	- Xác định các hạng mục được giám sát bởi hệ thống và các hạng mục được giám sát bởi người sử dụng. - Kiểm tra sự không nhất quán giữa thông tin đã đăng ký và tình trạng sử dụng của người sử dụng. - Giải thích cho người sử dụng về sự cần thiết của các nội dung cần được người sử dụng giám sát. - Báo cáo cho lãnh đạo các kết quả phân tích, đánh giá hiện trạng và các vấn đề về quản lý người sử dụng.				
SMSS 2.3	Quản lý vận hành					
	- Lĩnh vực hoạt động của tổ chức. - Quy tắc vận hành. - Quản lý lỗi và khắc phục lỗi. - Các điều kiện ràng buộc và các điểm cần xem xét để chuẩn bị lập kế hoạch. - Quản lý nhân sự. - Hợp đồng với nhân viên bên ngoài.	- Đánh giá khối lượng công việc và số lượng nhân viên theo yêu cầu. - Xác định công việc phù hợp với phạm vi ứng dụng CNTT. - Kiểm tra việc vận hành có được thực hiện chính xác, kịp thời theo thẩm quyền hay không. - Phân tích kết quả vận hành và đề xuất các biện pháp cải tiến cách thức vận hành hệ thống. - Vận hành và xây dựng các quy tắc làm việc nhóm để có hiệu suất cao nhất.				
SMSS 2.4	Quản lý chi phí					
	- Các phương pháp xác định ngân sách. - Các phương pháp thu thập thông tin về chi phí thực tế. - Chi phí ban đầu và chi phí vận hành. - Thuê và cho thuê. - Các phương pháp về chi phí bổ sung. - Hợp đồng và thanh toán hợp đồng. - Các phương pháp phân tích sự	- Chia các hạng mục chi phí theo nguồn vốn và loại chi. - Xem xét việc mua sắm một cách thích hợp bằng cách so sánh giữa việc mua sắm và thuê ngoài. - Xác định sự phù hợp giữa ngân sách và chi tiêu thực tế. - Phân tích sự khác biệt giữa ngân sách và chi tiêu thực tế và báo các kết quả phân tích cho lãnh đạo.				

Mã tham chiếu	Nội dung/ Yêu cầu cần đạt		Yêu cầu cần đạt theo hạng			
	Kiến thức	Kỹ năng	4	3	2	1
	khác biệt giữa ngân sách và chi tiêu thực tế.					
SMSS 2.5	Quản lý nhân lực					
	- Bộ Luật Lao động. - Pháp luật liên quan đến bình đẳng giới trong tuyển dụng và sử dụng lao động. - Pháp luật liên quan đến sức khỏe và an toàn lao động. - Giáo dục và đào tạo. - Hợp đồng bên ngoài. - Quản lý nhiệm vụ.	- Tính toán số giờ lao động cần thiết. - Tính toán chất lượng lao động. - Thiết lập các nhiệm vụ một cách thích hợp. - Quản lý trạng thái công việc và tình trạng sức khỏe của nhân viên. - Hỗ trợ nâng cao năng lực của nhân viên. - Điều chỉnh và đàm phán giữa các tổ chức để luân chuyển cán bộ. - Điều chỉnh và đàm phán với các nhà thầu bên ngoài để sắp xếp nhân viên.				
SMSS 2.6	Quản lý các điểm phân tán (Distributed site)					
	- Các vấn đề về quản lý hệ thống tại các điểm phân tán. - Cấu hình hệ thống và các cấu phần của các điểm phân tán. - Công việc của người sử dụng các điểm phân tán. - Các công nghệ về hệ thống phân tán.	- Nắm bắt các yêu cầu về quản lý vận hành hệ thống tại các điểm phân tán. - Xây dựng hệ thống quản lý các điểm phân tán trên cơ sở kế hoạch quản lý hệ thống. - Nắm bắt các vấn đề về quản lý vận hành hệ thống phân tán và xem xét các biện pháp khắc phục. - Xây dựng kế hoạch đào tạo tại các điểm phân tán.				
SMSS 2.7	Sử dụng hệ thống quản lý vận hành					
	- Các công việc chung trong vận hành hệ thống. - Hệ thống quản lý vận hành. - Các yêu cầu đối với hệ thống hóa. - Các gói phần mềm có sẵn dùng trong quản lý vận hành.	- Nắm bắt các vấn đề về quản lý vận hành hệ thống và đề xuất cải tiến. - Định lượng các tác động của việc ứng dụng hệ thống quản lý vận hành. - Xác định khả năng thích ứng của gói phần mềm cho các công việc của tổ chức. - Đề xuất giải pháp khắc phục các vấn đề liên quan đến việc				

Mã tham chiếu	Nội dung/ Yêu cầu cần đạt		Yêu cầu cần đạt theo hạng			
	Kiến thức	Kỹ năng	4	3	2	1
		quản lý hệ thống phân tán.				
SMSS 2.8	Chuẩn hóa					
	- Các công việc liên quan đến vận hành hệ thống. - Thủ tục chuẩn hóa. - Quản lý các chuẩn.	- Xây dựng các biểu mẫu cố định và chung cho các công việc. - Xây dựng tài liệu về vận hành và chuẩn hóa để hướng dẫn cho người sử dụng. - Xây dựng các chuẩn về khối lượng công việc và giải thích cho người sử dụng về các chuẩn này. - Khả năng giải thích cho người sử dụng về sự cần thiết tuân thủ các chuẩn. - Nắm bắt thực trạng các công việc có thể ứng dụng CNTT và xác mức độ phù hợp theo các chuẩn.				
SMSS 3	**Mô đun: Quản lý tài nguyên**		**x**	**x**	**x**	**x**
SMSS 3.1	Quản lý phần cứng và tài nguyên mạng					
	- Phần cứng và mạng. - Tổng thể về cấu hình phần cứng và mạng, các thành phần cấu hình phần cứng và cấu hình mạng. - Thiết bị thông tin liên lạc và dịch vụ truyền thông. - Quản lý đăng ký. - Quản lý tài sản. - Quản lý cấu hình. - Quản lý thay đổi. - Bảo trì phần cứng. - Quản lý và bảo trì mạng. - Thủ tục kiểm tra mạng.	- Xây dựng bản đăng ký quản lý - Quản lý tài sản phần cứng và thành phần mạng thích hợp. - Quản lý tài sản phần cứng và tài sản mạng hiện có để duy trì các giá trị sử dụng. - Xác định phạm vi ảnh hưởng đối với vận hành liên quan đến sự thay đổi cấu hình phần cứng và mạng. - So sánh hiệu quả kinh tế giữa các hình thức sở hữu (mua, thuê và cho thuê). - Quản lý tài sản mạng hiện có để duy trì các giá trị sử dụng. - Đánh giá sự tương thích của các hệ thống truyền thông thành phần, thiết bị mạng và phần mềm mạng cho tổ chức trên quan điểm vận hành. - So sánh hiệu quả kinh tế của các hệ thống thông tin liên lạc khác nhau.				

Mã tham chiếu	Nội dung/ Yêu cầu cần đạt		Yêu cầu cần đạt theo hạng			
	Kiến thức	Kỹ năng	4	3	2	1
SMSS 3.2	Quản lý phần mềm					
	- Phần mềm. - Cấu hình phần mềm. - Các yếu tố cấu hình phần mềm. - Việc quản lý đăng ký. - Quản lý cấu hình. - Quản lý thay đổi. - Vòng đời phần mềm. - Hợp đồng bản quyền phần mềm. - Việc hỗ trợ của nhà cung cấp phần mềm. - Bản quyền. - Các công cụ quản lý thư viện. - Các công cụ quản lý tài liệu.	- Xây dựng bản đăng ký quản lý và quản lý tài sản phần mềm một cách thích hợp. - Đánh giá khả năng tương thích của từng gói phần mềm thành phần đối với tổ chức theo quan điểm vận hành. - Xác định phạm vi ảnh hưởng của sự thay đổi cấu hình phần mềm đối với vận hành hệ thống. - So sánh sự khác biệt về yêu cầu bảo vệ quyền sở hữu trí tuệ do sự khác biệt trong hình thức phát triển (tự phát triển, phát triển theo cam kết và mua phần mềm).				
SMSS 3.3	Quản lý dữ liệu					
	- Dữ liệu của tổ chức. - Chính sách bảo mật dữ liệu của tổ chức. - Quản lý tài nguyên thông tin. - Vòng đời của dữ liệu. - Quản lý dữ liệu. - Hệ quản trị CSDL. - Quản lý CSDL. - Danh mục hệ thống (catalog). - Từ điển/ thư mục dữ liệu. - Chuẩn hóa dữ liệu. - Thủ tục kiểm soát dữ liệu.	- Xác định tầm quan trọng của dữ liệu. - Đánh giá sự tương thích của các công cụ quản lý an toàn, quản lý dữ liệu, công cụ phân tích dữ liệu từ quan điểm vận hành. - Giải thích các số liệu và phối hợp với kiểm soát viên.				
SMSS 3.4	Quản lý trang thiết bị					
	- Các tòa nhà của tổ chức và trang thiết bị phụ trợ. - Trang thiết bị vận hành máy tính. - Trang thiết bị truyền thông. - Pháp luật liên quan đến các biện pháp an toàn cho các cơ sở vật chất và trang thiết bị. - Các hình thức sở hữu cơ sở vật chất và thiết bị (mua, cho thuê và thuê).	- Xác định được tầm quan trọng của thiết bị. - Nắm bắt các điểm cần lưu ý trong quản lý thiết bị. - Nắm bắt nhược điểm của quy trình quản lý thiết bị và thực hiện các biện pháp đề phòng cần thiết. - So sánh hiệu quả kinh tế của các hình thức sở hữu khác nhau (mua, cho thuê và thuê). - Nắm bắt nhược điểm của các				

Mã tham chiếu	Nội dung/ Yêu cầu cần đạt		Yêu cầu cần đạt theo hạng			
	Kiến thức	Kỹ năng	4	3	2	1
	- Bảo hiểm thiệt hại. - Tiêu chuẩn và biện pháp bảo đảm an toàn hệ thống thông tin.	tòa nhà nơi lắp đặt thiết bị, của trang thiết bị tại các địa điểm phân tán và thực hiện các biện pháp dề phòng cần thiết.				
SMSS 4	**Mô đun: Quản lý lỗi và sự cố**			x	x	x
SMSS 4.1	Giám sát lỗi					
	- Các nội dung cần giám sát. - Hệ thống giám sát. - Các loại lỗi hệ thống và các đặc trưng riêng lẻ. - Phương pháp phát hiện lỗi. - Các trường hợp lỗi trong quá khứ.	- Xây dựng phương pháp phát hiện lỗi từ giai đoạn đầu. - Xây dựng hình thức giám sát trong hoạt động giám sát. - Phân biệt các dấu hiệu của lỗi. - Xác định dấu hiệu của lỗi liệu có dẫn đến sự xuất hiện của lỗi hay không. - Xác định mức độ nghiêm trọng của lỗi đã xảy ra. - Xác định ảnh hưởng của lỗi tới nghiệp vụ của tổ chức.				
SMSS 4.2	Xác định nguyên nhân lỗi					
	- Các loại lỗi hệ thống và đặc điểm của lỗi. - Các phương pháp phân tích các yếu tố của lỗi. - Các trường hợp lỗi trong quá khứ.	- Lập và thực hiện kế hoạch đào tạo để cô lập lỗi ở giai đoạn đầu và điều tra nguyên nhân. - Chỉ định nhân viên thích hợp để điều tra nguyên nhân theo đặc điểm lỗi và sự hợp tác của những người khác. - Khoanh vùng phạm vi ảnh hưởng của lỗi. - Xác định trạng thái lỗi và khởi động lại hệ thống một cách thích hợp.				
SMSS 4.3	Xử lý, khôi phục hệ thống					
	- Quy trình khôi phục dữ liệu. - Quy trình khôi phục mạng. - Việc khôi phục phần cứng và phần mềm. - Các loại lỗi và phân loại lỗi. - Việc đánh giá các biện pháp phòng ngừa chống tái diễn lỗi.	- Xây dựng phương pháp khôi phục ít ảnh hưởng đến người sử dụng. - Đưa ra nhiều phương pháp khôi phục và chọn phương pháp tối ưu. - Lựa chọn người thích hợp theo nội dung công việc khôi phục. - Xây dựng và thực hiện kế hoạch đào tạo về khôi phục. - Mô tả lỗi theo đặc tả một cách				

Mã tham chiếu	Nội dung/ Yêu cầu cần đạt		Yêu cầu cần đạt theo hạng			
	Kiến thức	Kỹ năng	4	3	2	1
		chính xác và hiệu quả. - Phân tích nguyên nhân gây lỗi một cách đầy đủ và thực hiện những hành động để ngăn chặn tái diễn. - Dự đoán các lỗi có thể xảy ra trong môi trường của tổ chức. - Đánh giá kết quả thực tế của các biện pháp phòng ngừa chống tái diễn lỗi.				
SMSS 5	**Mô đun: Quản lý an toàn thông tin cho hệ thống**			x	x	x
SMSS 5.1	Thiết lập hệ thống quản lý và chính sách an toàn thông tin					
	- Các yêu cầu an toàn thông tin. - Kế hoạch đối phó với trường hợp bất ngờ. - Các nguy cơ tiềm ẩn. - Các công cụ quản lý an toàn thông tin. - Cơ sở dữ liệu. - Mạng. - Các biện pháp an toàn thông tin vật lý, kỹ thuật và quản lý. - Pháp luật liên quan đến an toàn thông tin. - Trường hợp an toàn thông tin bị xâm phạm. - Công nghệ an toàn thông tin và các tình huống sử dụng. - Chi phí về kỹ thuật cho các biện pháp an toàn thông tin.	- Xác định khả năng mất an toàn thông tin trong tổ chức. - Tìm hiểu chính sách an toàn thông tin của các tổ chức và biện pháp an toàn thông tin được xây dựng trong hệ thống. - Đánh giá rủi ro. - Tính toán tỷ lệ chi phí/ lợi ích cho các biện pháp an toàn thông tin. - Xây dựng kế hoạch an toàn thông tin vật lý, kỹ thuật, quản lý và thực hiện kế hoạch.				
SMSS 5.2	Giám sát xâm nhập an toàn thông tin và phân tích trạng thái					
	- Các dạng xâm nhập an toàn thông tin và đặc điểm của từng dạng. - Kỹ thuật để phát hiện sự xâm nhập an toàn thông tin. - Các trường hợp xâm nhập an toàn thông tin trong quá khứ. - Việc thực hiện các biện pháp chống lại sự xâm nhập an toàn thông tin. - Việc giám sát hệ thống thông tin. - Phần mềm kiểm tra an toàn	- Phân biệt các dấu hiệu của xâm nhập an toàn thông tin. - Xác định dấu hiệu có thể dẫn đến khả năng xâm nhập an toàn thông tin. - Xác định mức độ nghiêm trọng xâm nhập an toàn thông tin. - Xác định mức độ ảnh hưởng xâm nhập an toàn thông tin tới các bộ phận nghiệp vụ của tổ chức.				

Mã tham chiếu	Nội dung/ Yêu cầu cần đạt		Yêu cầu cần đạt theo hạng			
	Kiến thức	Kỹ năng	4	3	2	1
	thông tin.					
SMSS 5.3	Kiểm tra mức độ an toàn thông tin					
	- Phần mềm an toàn thông tin. - Danh sách kiểm tra mức độ an toàn thông tin.	- Nắm bắt được tầm quan trọng của việc kiểm tra xác nhận mức độ an toàn thông tin. - Nắm bắt nội dung các mục trong danh sách kiểm tra mức độ an toàn thông tin và các tiêu chí chấp nhận. - Xác định hiệu quả phương pháp kiểm tra mức độ an toàn thông tin.				
SMSS 6	**Mô đun: Quản lý hiệu năng hệ thống**			x	x	x
SMSS 6.1	Đánh giá hiệu năng hệ thống					
SMSS 6.1.1	Thiết lập tiêu chí đánh giá hiệu năng					
	- Mô hình giám sát hiệu năng. - Đặc tả hiệu năng phần cứng. - Phương pháp đánh giá hiệu năng. - Cấu hình hệ thống. - Mạng.	- Kết hợp các mô hình đánh giá hiệu năng hiện tại hoặc mới để thiết lập mô hình đánh giá hiệu năng theo các đặc trưng của tổ chức. - Thiết lập một giá trị mục tiêu ứng với các cấp độ dịch vụ trong mỗi chỉ số đánh giá hiệu năng. - Lựa chọn phương pháp thu thập dữ liệu phù hợp cho mỗi chỉ số đánh giá hiệu năng. - Xác định điểm nút cổ chai bằng cách phân tích dữ liệu hiệu năng.				
SMSS 6.1.2	Phân tích và đánh giá hiệu năng					
	- Các thông tin được sử dụng làm chỉ số đánh giá hiệu năng phần cứng, phần mềm, mạng và phương pháp thu thập các thông tin đó; các giá trị chuẩn. - Các thông tin được sử dụng làm chỉ số đánh giá hiệu năng tổng thể, các giá trị tiêu chuẩn và phương pháp thu thập. - Các công cụ đo lường hiệu năng. - Thống kê.	- Xác định biện pháp cải tiến khi kết quả đánh giá thấp hơn so với giá trị mục tiêu. - Lựa chọn các công cụ đo lường hiệu năng phù hợp với yêu cầu của tổ chức.				
SMSS 6.2	Quản lý năng lực hệ thống					

Mã tham chiếu	Nội dung/ Yêu cầu cần đạt		Yêu cầu cần đạt theo hạng			
	Kiến thức	**Kỹ năng**	**4**	**3**	**2**	**1**
	- Sự hạn chế của các nguồn tài nguyên. - Quan hệ giữa tài nguyên và hiệu năng. - Năng lực hệ thống. - Việc vận hành hệ thống ở công suất/ hiệu suất giới hạn. - Những thay đổi trong môi trường nghiệp vụ của người sử dụng.	- Tư vấn sử dụng hợp lý tài nguyên hệ thống. - Ước lượng tải hệ thống, dự đoán năng lực và hiệu năng giới hạn một cách chính xác và ngăn ngừa vấn đề phát sinh. - Phân tích nguyên nhân giảm hiệu năng từ nhiều góc độ khác nhau. - Đề xuất một cách hợp lý việc bổ sung thiết bị và đổi mới hệ thống, có tính đến tỷ lệ chi phí/ lợi ích. - Dự đoán những thay đổi trong trạng thái sử dụng hệ thống từ những thay đổi trong môi trường nghiệp vụ của người sử dụng.				
SMSS 7	**Mô đun: Bảo trì hệ thống**		**x**	**x**	**x**	**x**
SMSS 7.1	Xây dựng kế hoạch bảo trì hệ thống					
SMSS 7.1.1	Thu thập yêu cầu về bảo trì hệ thống					
	- Việc bảo trì phần cứng và phần mềm. - Bảo trì cơ sở vật chất và trang thiết bị.	- Lựa chọn nguồn thông tin về nhu cầu bảo trì. - Sắp xếp nhu cầu bảo trì. - Phân tích nhu cầu bảo trì. - Thiết lập mức độ ưu tiên các nhu cầu bảo trì.				
SMSS 7.1.2	Lập kế hoạch bảo trì hệ thống					
	- Việc bảo trì. - Các tổ chức chịu trách nhiệm bảo trì hệ thống. - Bảo trì phần cứng và phần mềm. - Hợp đồng bảo trì phần mềm. - Kế hoạch nâng cấp của các nhà cung cấp phần mềm. - Quản lý thay đổi phần mềm. - Bảo trì mạng. - Cơ sở vật chất và trang thiết bị.	- Thực hiện kế hoạch bảo trì đáp ứng nhu cầu của người sử dụng. - Phân biệt phạm vi ảnh hưởng của việc thực hiện bảo trì đối với người sử dụng.				
SMSS 7.2	Thực hiện bảo trì hệ thống					
	- Quy trình bảo trì hệ thống. - Quản lý thay đổi phần mềm. - Bảo trì phần mềm.	- Giảm thiểu phạm vi ảnh hưởng của việc bảo trì đối với công việc của người sử dụng.				

Mã tham chiếu	Nội dung/ Yêu cầu cần đạt		Yêu cầu cần đạt theo hạng			
	Kiến thức	**Kỹ năng**	**4**	**3**	**2**	**1**
	- Phân phối phần mềm. - Hợp đồng bảo trì.	- Quyết định biện pháp cải tiến ngăn ngừa các vấn đề phát sinh trong quá trình thực hiện bảo trì. - Xem xét ảnh hưởng của việc nâng cấp phần mềm. - Đàm phán với các nhà cung cấp phần mềm. - Đàm phán với các nhà thầu bên ngoài để phát triển phần mềm. - Xác định sự cần thiết phải bảo trì. - Thực hiện kế hoạch bảo trì.				
SMSS 8	**Mô đun: Xây dựng hệ thống mới và di chuyển hệ thống (system migration)**			**x**	**x**	**x**
SMSS 8.1	Xây dựng kế hoạch phát triển hệ thống					
	- Phát triển hệ thống. - Bảo trì hệ thống. - Kiểm thử hệ thống. - Di chuyển hệ thống	- Đề xuất việc cải tiến trong quá trình phát triển hệ thống trên quan điểm quản lý vận hành hệ thống. - Xây dựng kế hoạch vận hành hệ thống và đạt được được sự chấp thuận. - Đánh giá khả năng thực hiện các yêu cầu quản lý vận hành hệ thống. - Đàm phán và điều chỉnh với những người liên quan về việc phát triển hệ thống.				
SMSS 8.2	Thiết kế phương pháp vận hành hệ thống					
	- Kiến trúc máy tính. - Quản lý hệ thống. - Các vấn đề liên quan đến quản lý vận hành thực tế tại tổ chức. - Các xu thế về công nghệ quản lý vận hành. - Các công cụ quản lý vận hành có trên thị trường.	- Xác định các biện pháp giải quyết vấn đề về quản lý vận hành phù hợp với thực tế của tổ chức. - Đánh giá sự tương thích của các phương pháp quản lý vận hành.				
SMSS 8.3	Thử nghiệm vận hành và di chuyển hệ thống					
	- Các công cụ kiểm thử. - Vận hành hệ thống.	- Lựa chọn các hạng mục có thể áp dụng trong thử nghiệm di chuyển hệ thống. - Lựa chọn các công cụ thử				

Mã tham chiếu	Nội dung/ Yêu cầu cần đạt		Yêu cầu cần đạt theo hạng			
	Kiến thức	Kỹ năng	4	3	2	1
		nghiệm trong quá trình di chuyển hệ thống. - Dự kiến các công việc khi di chuyển hệ thống. - Xác định sự phù hợp của sự vận hành hệ thống và khôi phục hệ thống dự phòng.				
SMSS 8.4	Di chuyển hệ thống					
	- Các hệ thống mới và cũ. - Các công cụ di chuyển. - Di chuyển dữ liệu. - Các vấn đề liên quan đến di chuyển trong quá khứ.	- Giảm thiểu các ảnh hưởng liên quan đến di chuyển hệ thống đối với người sử dụng. - Giải thích cho các người có liên quan về kế hoạch di chuyển hệ thống và điều chỉnh theo các ý kiến khác nhau. - Xác định liệu có tiếp tục di chuyển hệ thống trong quá trình thực hiện việc di chuyển.				
SMSS 8.5	Quản lý môi trường phát triển					
	- Cấu hình hệ thống. - Phát triển hệ thống. - Môi trường phát triển và các đặc điểm của người sử dụng.	- Duy trì trạng thái cho phần hệ thống không thay đổi so với hệ thống hiện tại. - Duy trì trạng thái cho phần hệ thống không ảnh hưởng đến hệ thống khác. - Duy trì trạng thái cho phần hệ thống bị lỗi nhưng có thể xử lý được nếu xảy ra trong hệ thống mới. - Điều chỉnh nguồn lực theo tiến độ phát triển hệ thống. - Đàm phán và điều chỉnh theo người sử dụng môi trường phát triển.				
SMSS 9	**Mô đun: Đánh giá hoạt động của hệ thống**				**x**	**x**
SMSS 9.1	Xác định mục tiêu đánh giá và các mục cần đánh giá					
	- Công việc quản lý vận hành. - Tài nguyên hệ thống thông tin. - Vòng đời hệ thống.	- Đánh giá mục tiêu vận hành ở giai đoạn thiết kế hệ thống. - Đánh giá hệ thống vận hành, hiệu năng và công suất ở giai đoạn thiết kế hệ thống. - Đánh giá chức năng, hiệu quả và độ tin cậy trong giai đoạn di chuyển hệ thống. - Đánh giá hiệu quả tổng thể				

Mã tham chiếu	Nội dung/ Yêu cầu cần đạt		Yêu cầu cần đạt theo hạng			
	Kiến thức	Kỹ năng	4	3	2	1
		của hệ thống trong giai đoạn vận hành hệ thống.				
SMSS 9.2	Thiết lập các hạng mục, tiêu chí đánh giá và thực hiện đánh giá					
	- Quản lý vận hành hệ thống. - Tài nguyên của hệ thống thông tin. - Các phương pháp đánh giá. - Giá trị tham khảo của các chỉ số đánh giá.	- Xác định sự hợp lý của các tiêu chí đánh giá. - Phân tích các yếu tố trong các trường hợp kết quả đánh giá thấp hơn so với mục tiêu.				
SMSS 9.3	Đề xuất cải tiến hệ thống					
	- Công việc đánh giá cải tiến.	- Làm cho những người liên quan hiểu được đề xuất cải tiến. - Phân biệt nguyên nhân thực sự của vấn đề vận hành và quyết định các biện pháp giải quyết. - Nắm bắt các đề xuất phản biện. - Giải quyết các vấn đề chung.				
SMSS 10	**Mô đun: Hỗ trợ người sử dụng**		**x**	**x**	**x**	**x**
SMSS 10.1	Hỗ trợ người sử dụng					
	- Công việc của người sử dụng. - Trình độ kỹ thuật của người sử dụng. - Mối quan hệ giữa hành vi vi phạm quy tắc và lỗi. - Các phương pháp thu thập thông tin - Thông tin kỹ thuật và các tài liệu liên quan đến nhu cầu của người sử dụng.	- Xác định vấn đề nảy sinh trong quản lý vận hành hệ thống do vi phạm quy tắc. - Xây dựng và phổ biến quy tắc. - Nhận biết và phân tích nhu cầu của người sử dụng và cung cấp giải pháp để đáp ứng nhu cầu của người sử dụng. - Mô tả nội dung đào tạo một cách chính xác và đơn giản, giúp cho người sử dụng hiểu được. - Đánh giá năng lực của người sử dụng cần đào tạo và đặt mục tiêu đào tạo phù hợp. - Chuẩn bị nội dung đào tạo và môi trường đào tạo. - Hướng dẫn và tư vấn cho người sử dụng theo các mức độ hiểu biết và trình độ kỹ thuật.				
SMSS 10.2	Hỗ trợ người sử dụng khi phát sinh yêu cầu mới					
	- Phạm vi của dịch vụ. - Môi trường hệ thống và các yếu	- Phân biệt các yêu cầu của người sử dụng và mức ưu tiên				

Mã tham chiếu	Nội dung/ Yêu cầu cần đạt		Yêu cầu cần đạt theo hạng			
	Kiến thức	Kỹ năng	4	3	2	1
	tố thành phần. - Quy trình sử dụng các nguồn tài nguyên. - Việc điều tra mức độ hài lòng của người sử dụng.	tương ứng. - Tìm hiểu các vấn đề về công nghệ quản lý vận hành hệ thống. - Xác định biện pháp để cải thiện mức độ hài lòng của người sử dụng dưới quan điểm vận hành.				

PHỤ LỤC SỐ 05[7]
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 quét lỗ hổng và nhận biết lỗ hổng trong hệ thống bảo mật.				
	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 (tức là kiểm soát an toàn) của hệ thống thông tin và mạng.				

[7] Phụ lục này được thay thế theo quy định tại Điều 2 của Thông tư số 17/2021/TT-BTTTT ngày 30 tháng 11 năm 2021 của Bộ trưởng Bộ Thông tin và Truyền thông 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, có hiệu lực kể từ ngày 01 tháng 6 năm 2022.

Mã Tham	Mã	Kiến thức	Mã	Kỹ năng	4	3	2	1
	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.).				
	KT007	Kiến thức về phương pháp xác thực, ủy quyền và kiểm soát truy cập.	KN043	Kỹ năng nhận biết, phân loại lỗ hổng bảo mật 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 biện pháp 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, trò chơi hướng dẫn, 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 của cơ sở hạ tầng Kiểm tra & Đánh giá (con người, phạm vi, công cụ, thiết bị do dạc).				
	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 thử, tài nguyên kiểm thử và nhân sự kiểm thử để đảm bảo hoàn thành các sự kiện kiểm thử 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 an toàn thông tin				

Mã Tham	Mã	Kiến thức	Mã	Kỹ năng	4	3	2	1
	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 cơ sở hạ tầng phòng thủ không gian mạng và giải quyết vấn đề.				
	KT020	Kiến thức về hệ thống cơ sở dữ liệu.	KN068	Kỹ năng quản trị nhân lực cho việc vận hành hệ thống CNTT.				
	KT021	Kiến thức về kế hoạch duy trì hoạt động và khôi phục thảm họa.	KN072	Kỹ năng đánh giá 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 quản lý hệ thống mạng (ví dụ: giám sát hiệu suất hệ thống end-to-end) và các công cụ.				
	KT024	Kiến thức về kết nối Mạng cục bộ và mạng diện rộng của tổ chức.	KN075	Kỹ năng thực hiện đánh giá lỗ hổng bảo mật lớp 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.				

Mã Tham	Mã	Kiến thức	Mã	Kỹ năng	4	3	2	1
	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 đáp ứng các mục tiêu bảo mật 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.				
	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 mã hóa 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 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 mã.				
	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 đặc quyền quản trị.				
	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, bao gồm việc chuẩn bị các kế hoạch hỗ trợ chức năng và cụ thể, chuẩn bị và quản lý thư từ, và các thủ tục nhân sự.				
	KT071	Kiến thức về các nguyên tắc và phương pháp phân tích cấu trúc.	KN096	Kỹ năng phân tích mạng lưới liên lạc của mục tiêu.				

Mã Tham	Mã	Kiến thức	Mã	Kỹ năng	4	3	2	1
	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 lỗ hổng và hạn chế trí thông minh.				
	KT080	Kiến thức về kiến trúc công nghệ thông tin, Chính phủ điện tử.	KN107	Kỹ năng xác định các vấn đề ngôn ngữ có thể có 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.				
	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 mà 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.				

Mã Tham	Mã	Kiến thức	Mã	Kỹ năng	4	3	2	1
	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 quét lỗ hổng để xác định lỗ hổng.				
	KT162	Kiến thức về các tiêu chuẩn an toàn thông tin cá nhân, dữ liệu cá nhân.	KN117	Kỹ năng quản lý kiến thức, bao gồm các kỹ thuật tài liệu kỹ thuật (ví dụ: Wikipage).				
	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 mang lại kết quả chất lượng.				
	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 tra thâm 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.				

Mã Tham	Mã	Kiến thức	Mã	Kỹ năng	4	3	2	1
	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 hoạt động thu thập.				
			KN130	Kỹ năng xác định sự bất thường của mạng mục tiêu (ví dụ: xâm nhập, luồng dữ liệu hoặc xử lý, triển khai mục tiêu các công nghệ mới).				
			KN131	Kỹ năng viết kỹ thuật.				
			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 bao gồm duy trì 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 làm rõ ngành học để thu thập thông tin cần thiết.				

Mã Tham	Mã	Kiến thức	Mã	Kỹ năng	4	3	2	1
			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).				
			KN148	Kỹ năng sử dụng cấu trúc và quy trình báo cáo của giải pháp phòng thủ trên không gian mạng của riêng từng tổ chức				
			KN149	Kỹ năng xác định các vấn đề về an toàn thông tin mạng và quyền riêng tư xuất phát từ kết nối với các khách hàng và tổ chức đối tác bên trong và bên ngoài.				
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 mật thông tin liên lạc mạng.				

Mã Tham	Mã	Kiến thức	Mã	Kỹ năng	4	3	2	1
	KT004	Kiến thức về an toàn thông tin mạng và các nguyên tắc quyền riêng tư.	KN043	Kỹ năng nhận biết, phân loại lỗ hổng bảo mật 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 tương quan sự kiện an toàn thông tin.				
	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.						

Mã Tham	Mã	Kiến thức	Mã	Kỹ năng	4	3	2	1
	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.						
	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 những kẻ tấn công mạng (ví dụ: kẻ 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).						

Mã Tham	Mã	Kiến thức	Mã	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).						
	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.						
	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 quét lỗ hổng và nhận biết lỗ hổng trong hệ thống bảo mật.				

Mã Tham	Mã	Kiến thức	Mã	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).	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.).				
	KT009	Kiến thức về các điểm yếu ứng dụng.	KN046	Kỹ năng sử dụng các công cụ phân tích lỗ hổng mạng. (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 lỗ hổng bảo mật lớp 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				

Mã Tham	Mã	Kiến thức	Mã	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).	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,...).						
	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 những kẻ tấn công mạng (ví dụ: kẻ nghiệp dư (script kiddies), nội gián, tài trợ quốc gia,...).						

Mã Tham	Mã	Kiến thức	Mã	Kỹ năng	4	3	2	1
	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).						
	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.						

Mã Tham	Mã	Kiến thức	Mã	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.						
	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 tra thâm 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)						
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.				

Mã Tham	Mã	Kiến thức	Mã	Kỹ năng	4	3	2	1
	KT004	Kiến thức về an toàn thông tin mạng và các nguyên tắc quyền riêng tư.	KN017	Kỹ năng kiểm tra, đánh giá lỗ hổng bảo mật từ khâu 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 lỗ hổng bảo mật và các hình thức tấn công liên quan.				
	KT015	Kiến thức về thuật toán máy tính.	KN056	Kỹ năng đọc và giải thích chữ ký (ví dụ: snort).				
	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.				
	KT020	Kiến thức về hệ thống cơ sở dữ liệu.	KN086	Kỹ năng nhận biết lỗ hổng trong hệ thống bảo mật. (ví dụ: quét lỗ hổng bảo mật và 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				

Mã Tham	Mã	Kiến thức	Mã	Kỹ năng	4	3	2	1
				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 cấu trúc và quy trình báo cáo của giải pháp phòng thủ trên không gian mạng của riêng từng tổ chức				
	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).						
	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						

Mã Tham	Mã	Kiến thức	Mã	Kỹ năng	4	3	2	1
		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,...).						
	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.						

Mã Tham	Mã	Kiến thức	Mã	Kỹ năng	4	3	2	1
	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.						
	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 những kẻ tấn công mạng (ví dụ: kẻ nghiệp dư (script kiddies), nội gián, tài trợ quốc gia,...).						
	KT117	Kiến thức về kỹ thuật quản trị hệ thống, mạng và						

Mã Tham	Mã	Kiến thức	Mã	Kỹ năng	4	3	2	1
		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.						
	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).						

Mã Tham	Mã	Kiến thức	Mã	Kỹ năng	4	3	2	1
	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).						
	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.						

Mã Tham	Mã	Kiến thức	Mã	Kỹ năng	4	3	2	1
	KT208	Kiến thức về các nguyên tắc, công cụ và kỹ thuật kiểm tra thâm 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.				
	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.				
	KT004	Kiến thức về an toàn thông tin mạng và các nguyên tắc quyền riêng tư.	KN027	Kỹ năng sử dụng thiết bị và mã hóa Mạng riêng ảo (VPN).				
	KT005	Kiến thức về các mối đe dọa và điểm yếu an toàn thông tin mạng.	KN042	Kỹ năng bảo mật thông tin liên lạc mạng.				
	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 kỹ thuật tăng cường 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.).				

Mã Tham	Mã	Kiến thức	Mã	Kỹ năng	4	3	2	1
	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.						
	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.						

Mã Tham	Mã	Kiến thức	Mã	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).						
	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).						
	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 thử và thực hiện các kế hoạch dự phòng, khôi phục cơ sở 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	KN030	Kỹ năng phân tích kết xuất bộ nhớ để trích xuất				

Mã Tham	Mã	Kiến thức	Mã	Kỹ năng	4	3	2	1
		đức nghề nghiệp liên quan đến an toàn thông tin mạng và quyền riêng tư.		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 truyền thông 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 thành phần hệ thống áp dụng 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 chất 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.				
	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 PC.				
	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 sâu về mã độc hại đã thu được (ví dụ: điều tra về phần mềm độc hại).				
	KT066	Kiến thức về các công cụ đánh giá máy chủ và	KN050	Kỹ năng sử dụng các công cụ phân tích nhị phân				

Mã Tham	Mã	Kiến thức	Mã	Kỹ năng	4	3	2	1
		kỹ thuật xác định lỗi.		(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 an toàn [SHA], Thuật toán tiêu hóa tin nhắn [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				
	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.				
	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 phần mềm độc hại.				
	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 kỹ thuật 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.				
	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.						

Mã Tham	Mã	Kiến thức	Mã	Kỹ năng	4	3	2	1
	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.						
	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 phụ 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).						

Mã Tham	Mã	Kiến thức	Mã	Kỹ năng	4	3	2	1
	KT133	Kiến thức về các quy trình và công cụ gỡ lỗi.						
	KT134	Kiến thức về việc lạm dụng loại tệp bởi kẻ địch đối với 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.						
	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**

Mã Tham	Mã	Kiến thức	Mã	Kỹ năng	4	3	2	1
	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.				
	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 mã hóa 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.						

Mã Tham	Mã	Kiến thức	Mã	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 mà 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.						
	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.						

Mã Tham	Mã	Kiến thức	Mã	Kỹ năng	4	3	2	1
	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.						
	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 tra thâm nhập.						
	KT235	Kiến thức về an toàn hoạt động.						
CSSS 8	**Đánh giá an toàn phần mềm**				**x**	**x**	**x**	**x**

Mã Tham	Mã	Kiến thức	Mã	Kỹ năng	4	3	2	1
	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 quét lỗ hổng và nhận biết lỗ hổng trong hệ thống bảo mật.				
	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 xây dựng, áp dụng các biện pháp đối phó với các rủi ro an toàn thông tin.				
	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 truy cập hệ thống bảo mật.				
	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 (tức là 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 bảo mật hộp đen vào quy trình đảm bảo chất lượng của các bản phát hành phần mềm.				
	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: đơn vị, tích hợp, hệ thống, chấp nhận).				
	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 mã.				
	KT022	Kiến thức về kiến trúc an toàn thông tin của tổ chức.	KN094	Kỹ năng thực hiện phân tích đặc quyền quản trị.				

Mã Tham	Mã	Kiến thức	Mã	Kỹ năng	4	3	2	1
	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.						
	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.						

Mã Tham	Mã	Kiến thức	Mã	Kỹ năng	4	3	2	1
	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.				
	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 xây dựng, áp dụng các biện pháp đối phó với các rủi ro an toàn thông tin.				
	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 lập mô hình thiết kế và xây dựng các trường hợp sử dụng (ví dụ: ngôn ngữ lập mô hình unifie).				

Mã Tham	Mã	Kiến thức	Mã	Kỹ năng	4	3	2	1
	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 và mã hóa Mạng riêng ảo (VPN).				
	KT007	Kiến thức về phương pháp xác thực, ủy quyền và kiểm soát truy cập.	KN029	Kỹ năng viết kế hoạch kiểm thử.				
	KT008	Kiến thức về áp dụng các quy trình kinh doanh và hoạt động của các tổ chức.	KN041	Kỹ năng cài đặt. cấu hình các phần mềm, công cụ bảo vệ máy tính. (ví dụ: tường lửa phần mềm, 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 bảo mật đa cấp / tên miền chéo.				
	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.				
	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 hoạt động thành nhu cầu bảo vệ (tức là kiểm soát an toàn).				
	KT015	Kiến thức về thuật toán máy tính.	KN087	Kỹ năng thiết lập mạng con vật lý hoặc logic để tách mạng cục bộ (LAN) khỏi các mạng không đáng tin cậy khác.				

Mã Tham	Mã	Kiến thức	Mã	Kỹ năng	4	3	2	1
	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 phần cứng, 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						
	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).						

Mã Tham	Mã	Kiến thức	Mã	Kỹ năng	4	3	2	1
	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.						
	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.						

Mã Tham	Mã	Kiến thức	Mã	Kỹ năng	4	3	2	1
	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 mà 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.						
	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.						

Mã Tham	Mã	Kiến thức	Mã	Kỹ năng	4	3	2	1
	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.						
	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: dường 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						

Mã Tham	Mã	Kiến thức	Mã	Kỹ năng	4	3	2	1
		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.						
	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 quét lỗ hổng và nhận biết lỗ hổng trong hệ thống bảo mật.				
	KT002	Kiến thức về các quy trình quản lý rủi ro (ví dụ:	KN009	Kỹ năng xây dựng, áp dụng các biện pháp đối				

Mã Tham	Mã	Kiến thức	Mã	Kỹ năng	4	3	2	1
		các phương pháp đánh giá và giảm thiểu rủi ro).		phó với các rủi ro an toàn thông tin.				
	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 xây dựng các biện pháp kiểm soát bảo mật an toàn thông tin.				
	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 truy cập hệ thống bảo mật.				
	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 (tức là kiểm soát an toàn) của hệ thống thông tin và mạng.				
	KT015	Kiến thức về thuật toán máy tính.	KN017	Kỹ năng kiểm tra, đánh giá lỗ hổng bảo mật từ khâu thiết kế.				
	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 đáp ứng các mục tiêu bảo mật 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).				
	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).						

Mã Tham	Mã	Kiến thức	Mã	Kỹ năng	4	3	2	1
	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						
	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.						

Mã Tham	Mã	Kiến thức	Mã	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.						
	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.						
	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.						

Mã Tham	Mã	Kiến thức	Mã	Kỹ năng	4	3	2	1
	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.						
	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 mà 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).						

Mã Tham	Mã	Kiến thức	Mã	Kỹ năng	4	3	2	1
	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.						
	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.						

Mã Tham	Mã	Kiến thức	Mã	Kỹ năng	4	3	2	1
	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 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 truy cập hệ thống bảo mật.				
	KT004	Kiến thức về an toàn thông tin mạng và các nguyên tắc quyền riêng tư.	KN017	Kỹ năng kiểm tra, đánh giá lỗ hổng bảo mật từ khâu 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.				

Mã Tham	Mã	Kiến thức	Mã	Kỹ năng	4	3	2	1
	KT017	Kiến thức về các thuật toán mã hóa	KN086	Kỹ năng nhận biết lỗ hổng trong hệ thống bảo mật. (ví dụ: quét lỗ hổng bảo mật và 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						
	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).						

Mã Tham	Mã	Kiến thức	Mã	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).						
	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.						
	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).						

Mã Tham	Mã	Kiến thức	Mã	Kỹ năng	4	3	2	1
	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.						
	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	Có 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.						

Mã Tham	Mã	Kiến thức	Mã	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.						
	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.						
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 phi quy kết.				
	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 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.				

Mã Tham	Mã	Kiến thức	Mã	Kỹ năng	4	3	2	1
	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 diễn giải, phân tích 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, bao hàm các yếu tố mục tiêu quan trọng cho miền 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.				
	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 Boolean để xây dựng các truy vấn đơn giản và phức tạp.				

Mã Tham	Mã	Kiến thức	Mã	Kỹ năng	4	3	2	1
	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 (ví dụ: Analyst's Notebook, A-Space, Anchory, M3, tư duy phân kỳ / hội tụ, biểu đồ liên kết, ma trận, v.v.).				
	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, LexisNexis, DataStar) và các công cụ trong việc thực hiện 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 không gian làm việc cộng tác ảo và / hoặc các công cụ (ví dụ: IWS, VTC, chat rooms, SharePoint).				
	KT216	Kiến thức về các bộ xâm nhập trên máy tính hiện hành.	KN137	Kỹ năng viết, đánh giá và chỉnh sửa các sản phẩm đánh giá / trí tuệ 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).						

Mã Tham	Mã	Kiến thức	Mã	Kỹ năng	4	3	2	1
	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).						
	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.						

Mã Tham	Mã	Kiến thức	Mã	Kỹ năng	4	3	2	1
	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.						
	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).						

Mã Tham	Mã	Kiến thức	Mã	Kỹ năng	4	3	2	1
	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.						

PHỤ LỤC SỐ 06
YÊU CẦU VỀ KIẾN THỨC, KỸ NĂNG CHUYÊN SÂU CỦA CHUẨN KỸ NĂNG THIẾT KẾ VÀ PHÁT TRIỂN PHẦN MỀM

(Ban hành kèm theo Thông tư số 11/2015/TT-BTTTT ngày 5/5/2015 của Bộ trưởng Bộ Thông tin và Truyền thông)

Mã tham chiếu	Nội dung/ Yêu cầu cần đạt		Yêu cầu cần đạt theo hạng			
	Kiến thức	Kỹ năng	4	3	2	1
SDSS 1	**Mô đun: Phân tích yêu cầu của người sử dụng và xác định yêu cầu hệ thống hóa**			x	x	x
SDSS 1.1	Thu thập và phân tích thông tin để xác định yêu cầu của người sử dụng					
	- Phạm vi và nội dung công việc của người sử dụng. - Các phương pháp thu thập thông tin. - Các phương pháp phân tích vấn đề.	- Xác định các nguồn thông tin chính về yêu cầu của người sử dụng. - Thực hiện các kỹ thuật và trình tự thu thập thông tin. - Xác định khối lượng thông tin cần thu thập. - Phân tích phản hồi từ các cá nhân và tập thể. - Lựa chọn, nhận các thông tin thu thập được và xác định nhu cầu. - Sắp xếp và tổng hợp thông tin về yêu cầu của người sử dụng. - Tạo môi trường thuận lợi để mọi người có thể trao đổi về các vấn đề quan trọng và đề xuất giải pháp. - Thu thập và trình bày dữ liệu về chi phí.				
SDSS 1.2	Xác định phạm vi công việc					
	- Môi trường hệ thống. - Kiến trúc hệ thống, phần cứng và mềm. - Tính hiện hữu của các tài nguyên và thời hạn bàn giao dự án. - Tính số giờ công. - Những hạn chế kỹ thuật. - Kỹ thuật phân tích rủi ro.	- Viết tài liệu về phạm vi yêu cầu của người sử dụng một cách rõ ràng. - Đàm phán với những người đặt hàng về tiêu chí cần đạt đối với dự án hệ thống hóa. - Ước tính số giờ công đối với mỗi mục công việc trong dự án hệ thống hóa. - Ước tính tiến độ hoàn thành của việc phát triển hệ thống. -Khảo sát, phân tích và so sánh các sản phẩm có trên thị trường và xác				

Mã tham chiếu	Nội dung/ Yêu cầu cần đạt		Yêu cầu cần đạt theo hạng			
	Kiến thức	Kỹ năng	4	3	2	1
		định khả năng áp dụng được đối với hệ thống. - Xây dựng tài liệu theo những ràng buộc về kỹ thuật. - Tư duy không theo tuần tự và tổng quan.				
SDSS 1.3	Xác định yêu cầu hệ thống hóa					
	- Hệ thống hóa và tích hợp hệ thống. - Các chức năng và vận hành của hệ thống. - Quy trình và năng lực phát triển.	- Chuyển yêu cầu người sử dụng thành yêu cầu của hệ thống. - Phát hiện các yêu cầu mâu thuẫn với nhau và trình bày giải pháp. - Phân tích tính đúng đắn và nhất quán của thông tin. - Áp dụng các công nghệ đáp ứng các yêu cầu một cách hiệu quả.				
SDSS 1.4	Xác định yêu cầu an toàn thông tin					
	- Rủi ro trong an toàn thông tin. - Chính sách an toàn thông tin của tổ chức. - Đảm bảo an toàn thông tin cho mạng. - Đảm bảo tính toàn vẹn của dữ liệu. - Các biện pháp bảo mật (kiểm soát truy nhập, mã hóa, xác thực, tường lửa) và các công cụ đảm bảo an toàn thông tin.	- Phân tích mức độ quan trọng của dữ liệu. - Xác định các loại rủi ro. - Chuyển các yêu cầu an toàn thông tin của người sử dụng thành yêu cầu an toàn thông tin của hệ thống. - Áp dụng công nghệ đáp ứng các yêu cầu về an toàn thông tin một cách hiệu quả.				
SDSS 1.5	Xác định yêu cầu vận hành					
	- Các yêu cầu vận hành hệ thống. - Biện pháp khắc phục lỗi hệ thống. - Các công cụ bảo trì.	- Chuyển yêu cầu vận hành của người sử dụng thành yêu cầu vận hành của hệ thống.				
SDSS 1.6	Xác định yêu cầu bảo trì					
	- Bảo trì hệ thống.	- Xác định các hạng mục mà người sử dụng yêu cầu bảo trì.				
SDSS 1.7	Thiết lập tiêu chí đánh giá hiệu năng					
	- Các yêu cầu hệ thống. - Xác định yêu cầu hiệu năng của hệ thống.	- Đánh giá tiêu chí đánh giá hiệu năng - Xác định khả năng đáp ứng tiêu chí đánh giá hiệu năng. - Đề xuất các hạng mục cần thiết để đảm bảo hiệu năng.				

Mã tham chiếu	Nội dung/ Yêu cầu cần đạt		Yêu cầu cần đạt theo hạng			
	Kiến thức	Kỹ năng	4	3	2	1
SDSS 1.8	Xác định yêu cầu kiểm thử					
	- Phương pháp kiểm thử. - Công cụ kiểm thử.	- Xác định các hạng mục kiểm thử đúng theo yêu cầu người sử dụng. - Kiểm tra việc thực hiện các yêu cầu hệ thống. - Xử lý các vấn đề khi kiểm thử.				
SDSS 1.9	Chuẩn bị và rà soát các tài liệu xác định yêu cầu					
	- Quy trình rà soát - Phát triển hệ thống và môi trường vận hành. - Các hạng mục và ghi chú cần đưa vào tài liệu xác định yêu cầu hệ thống.	- Mô tả một cách rõ ràng các hạng mục quan trọng. - Lựa chọn phương pháp trao đổi phù hợp để rà soát việc xác định yêu cầu và thúc đẩy tiến độ rà soát một cách hiệu quả. - Đánh giá các ý kiến trái ngược một cách phù hợp.				
SDSS 2	**Mô đun: Chuẩn bị phát triển hệ thống**			x	x	x
SDSS 2.1	Xác định mô hình vòng đời cho việc phát triển					
	- Các mô hình vòng đời phần mềm.	- Xác định quy mô, phạm vi, độ phức tạp của dự án. - Lựa chọn mô hình vòng đời phần mềm tương thích với dự án.				
SDSS 2.2	Chuẩn bị môi trường phát triển					
	- Phần cứng và phần mềm (công cụ, ngôn ngữ, phần mềm trung gian).	- Lựa chọn phần cứng và phần mềm tối ưu cho dự án (công cụ, ngôn ngữ, phần mềm trung gian).				
SDSS 2.3	Chuẩn bị kế hoạch thực hiện quy trình phát triển					
	- Chuẩn bị tài liệu kế hoạch dự án. - Quản lý rủi ro. - Động lực làm việc của nhân viên.	- Lập kế hoạch tối ưu, xem xét quy mô, độ phức tạp và nguồn lực để phát triển. - Trình bày mục tiêu của dự án. - Bố trí nhân sự hiệu quả. - Nắm được kỹ năng của nhân viên. - Động viên tinh thần nhân viên. - Nghiên cứu biện pháp phòng chống rủi ro.				
SDSS 3	**Mô đun: Thiết kế hệ thống (thiết kế ngoài)**				x	x
SDSS 3.1	Lựa chọn kiến trúc hệ thống					
	- Trình tự và kỹ thuật khảo sát. - Khái niệm và công nghệ thiết kế hệ thống. - Cân đối hệ thống (system trade-off).	- Xây dựng tài liệu chi tiết về kiến trúc hệ thống. - Đánh giá các phương án lập kế hoạch hệ thống hóa và giải thích cho những người có liên quan. - Xác định yêu cầu cốt lõi của hệ				

Mã tham chiếu	Nội dung/ Yêu cầu cần đạt		Yêu cầu cần đạt theo hạng			
	Kiến thức	Kỹ năng	4	3	2	1
	- Kiến trúc hệ thống, phần cứng và phần mềm. - Các tiêu chuẩn hệ thống hóa.	thống đối với kiến trúc hệ thống. - Thực hiện việc lựa chọn kỹ thuật có xem xét đến khía cạnh hiệu quả chi phí. - Giải thích tính phức tạp của hệ thống và phân tích các ý kiến của người sử dụng. - Thu thập, kết nối, và hiểu các số liệu.				
SDSS 3.2	Thiết kế đặc tả chức năng và giao diện cho các hệ thống con					
	- Hệ thống tổng thể. - Cấu trúc phân cấp của hệ thống.	- Phân tích và thiết lập sự nhất quán của hệ thống. - Phân rã hệ thống thành các hệ thống con. - Đánh giá tính phù hợp của các giao diện hệ thống con. - Thiết lập hệ thống một cách tối ưu. - Phân tích cấu hình hệ thống và tính ổn định.				
SDSS 3.3	Thiết kế an toàn thông tin					
	- Cách thiết kế yêu cầu an toàn thông tin. - Chính sách an toàn thông tin.	Áp dụng các công nghệ an toàn thông tin cho thiết kế hệ thống.				
SDSS 3.4	Xác định các công việc và mô hình dữ liệu					
	- Phương pháp luận phát triển mô hình công việc. - Phương pháp luận phát triển mô hình dữ liệu. - Kỹ thuật mô phỏng. - Hạn chế nghiệp vụ.	- Phát triển mô hình công việc và dữ liệu phù hợp với kỹ thuật phát triển mô hình. - Đánh giá dữ liệu. - Tạo mô hình mô phỏng. - Đánh giá tính nhất quán giữa nghiệp vụ và hệ thống. - Phân tích cấu trúc và kiến trúc hệ thống.				
SDSS 3.5	Chuẩn bị và rà soát tài liệu hướng dẫn người sử dụng (đề cương tài liệu hướng dẫn)					
	- Tiến trình rà soát tài liệu. - Công việc của người sử dụng. - Vận hành hệ thống. - Thiết kế giao diện đồ họa người sử dụng (GUI).	- Xây dựng tài liệu hướng dẫn sử dụng và các hạng mục cần mô tả. - Lựa chọn phương pháp trao đổi phù hợp để rà soát tài liệu hướng dẫn người sử dụng và cách thực hiện. - Đề xuất các phương án xây dựng giao diện người sử dụng phù hợp				

Mã tham chiếu	Nội dung/ Yêu cầu cần đạt		Yêu cầu cần đạt theo hạng			
	Kiến thức	Kỹ năng	4	3	2	1
		theo yêu cầu. - Sắp xếp, bố trí các yêu cầu vận hành (tài liệu và thao tác) khi hệ thống hóa công việc của người sử dụng.				
SDSS 3.6	Thiết kế đặc tả kiểm thử hệ thống					
	- Thiết kế đặc tả kiểm thử. - Công cụ kiểm thử. - Yêu cầu hệ thống.	- Thiết kế đặc tả kiểm thử phù hợp với khái niệm hệ thống hóa. - Chuẩn bị kế hoạch kiểm thử hệ thống. - Phân tích nguyên nhân và lý do của các vấn đề và trình bày kế hoạch hành động.				
SDSS 3.7	Chuẩn bị và rà soát tài liệu thiết kế hệ thống					
	- Các đặc tả hệ thống trong tài liệu. - Trình tự rà soát thiết kế và cách thực hiện. - Quy trình phát triển. - Môi trường vận hành.	- Hỗ trợ người sử dụng vốn không phải là kỹ sư hệ thống hiểu được đặc tả hệ thống một cách đúng đắn. - Giải thích các thông tin kỹ thuật liên quan đến hiệu quả của công việc. - Lựa chọn phương pháp trao đổi phù hợp với việc rà soát thiết kế hệ thống và thực hiện việc rà soát xét một cách hiệu quả. - Đánh giá các ý kiến đối lập một cách phù hợp.				
SDSS 4	**Mô đun: Thiết kế thành phần (thiết kế trong)**			**x**	**x**	**x**
SDSS 4.1	Thiết kế thành phần phần mềm					
	- Các kỹ thuật thiết kế phần mềm. - Các nền tảng có thể sử dụng được. - Thiết kế có cấu trúc. - Kỹ thuật thiết kế hướng đối tượng. - Tiêu chuẩn hóa. - Cấu hình hệ thống.	- Tìm hiểu đặc tả hệ thống và chia hệ thống con thành các thành phần. - Thiết kế giao diện giữa các thành phần một cách nhất quán. - Đảm bảo chất lượng theo yêu cầu. - Thực hiện các đặc tính như tính mở rộng, độ tin cậy và tính linh hoạt.				
SDSS 4.2	Thiết kế cơ sở dữ liệu mức vật lý					
	- Chuyển đổi mô hình dữ liệu logic thành mô hình dữ liệu vật lí. - Chuẩn hóa, phi chuẩn hóa, lý thuyết quan hệ, và các công cụ mô hình hóa dữ liệu.	- Thực hiện tốt các công việc liên quan đến xây dựng và vận hành cơ sở dữ liệu. - Tìm hiểu cấu trúc của mô hình logic và chuyển đổi chúng thành các cấu trúc dữ liệu thực.				

Mã tham chiếu	Nội dung/ Yêu cầu cần đạt		Yêu cầu cần đạt theo hạng			
	Kiến thức	Kỹ năng	4	3	2	1
	- Tính toán dung lượng của thiết bị lưu trữ và phân nhóm (clustering)	- Giải thích mối quan hệ giữa các mô hình dữ liệu và cơ sở dữ liệu. - Áp dụng các bước tạo cơ sở dữ liệu.				
SDSS 4.3	Tạo và kiểm thử bản chạy thử (prototype)					
	- Phương pháp luận thiết kế bản chạy thử. - Xây dựng bản chạy thử và các phương pháp kiểm thử. - Công cụ kiểm thử.	- Phân tích các điểm quan trọng. - Tích hợp các quan điểm về phần mềm và áp dụng để cải tiến hệ thống. - Đánh giá hiệu năng mô hình hệ thống trên cơ sở kết quả kiểm thử. - Đề xuất kế hoạch cải tiến. - Nhận thức được các hạn chế của phần mềm.				
SDSS 4.4	Thiết kế đặc tả kiểm thử thành phần					
	- Thiết kế đặc tả kiểm thử. - Công cụ kiểm thử. - Đặc tả thành phần và giao diện giữa các thành phần.	- Thiết kế đặc tả kiểm thử tương ứng với khái niệm thiết kế thành phần phần mềm. - Chuẩn bị kế hoạch kiểm thử thành phần. - Phân tích nguyên nhân và lý do của các vấn đề và trình bày kế hoạch hành động.				
SDSS 4.5	Rà soát thiết kế thành phần của phần mềm					
	- Tư liệu hóa đặc tả thành phần của phần mềm. - Trình tự rà soát thiết kế và thực hiện. - Quy trình phát triển. - Môi trường vận hành.	- Lựa chọn phương pháp trao đổi phù hợp với việc rà soát thiết kế thành phần và thực hiện việc rà soát một cách hiệu quả. - Giải thích logic thiết kế thành phần một cách rõ ràng. - Đánh giá các ý kiến đối lập. - Đề xuất các phương án khác. - Đề xuất kế hoạch tối ưu trên cơ sở nghiên cứu tổng thể.				
SDSS 5	**Mô đun: Thiết kế chi tiết (thiết kế chương trình)**			x	x	x
SDSS 5.1	Thực hiện thiết kế chi tiết phần mềm					
	- Thiết kế chi tiết phần mềm. - Các kỹ thuật viết câu để giải thích logic chương trình một cách đúng đắn. - Các công cụ CASE (Computer-Aided Software Engineering).	- Thiết kế đặc tả thành phần phần mềm một cách nhất quán. - Phân loại những vấn đề cần cân nhắc và chuẩn bị đặc tả chi tiết tương ứng. - Chọn lựa kỹ thuật thiết kế tối ưu. - Chọn lựa môi trường phát triển tối				

Mã tham chiếu	Nội dung/ Yêu cầu cần đạt		Yêu cầu cần đạt theo hạng			
	Kiến thức	Kỹ năng	4	3	2	1
	- Các ngôn ngữ lập trình.	ưu cho hệ thống.				
SDSS 5.2	Rà soát thiết kế chi tiết					
	- Tài liệu thiết kế chi tiết. - Trình tự rà soát một thiết kế và thực hiện. - Quy trình phát triển. - Môi trường thực hiện chương trình. - Môi trường vận hành.	- Lựa chọn phương pháp thông tin phù hợp và thực hiện rà soát thiết kế chi tiết. - Giải thích tính logic thiết kế chi tiết. - Đánh giá các ý kiến phản biện. - Tìm hiểu tình trạng triển khai chương trình và chỉ ra các vấn đề.				
SDSS 5.3	Thiết kế đặc tả kiểm thử đơn vị (unit)					
	- Thiết kế đặc tả kiểm thử đơn vị. - Các công cụ kiểm thử. - Quy trình sản xuất. - Môi trường vận hành. - Các ngôn ngữ lập trình. - Môi trường triển khai kiểm thử.	- Lập kế hoạch kiểm thử đơn vị. - Thực hiện kiểm thử, báo cáo lỗi, báo cáo chất lượng hệ thống phần mềm. - Thiết lập môi trường kiểm thử.				
SDSS 5.4	Chuẩn bị và rà soát tài liệu hướng dẫn người sử dụng (phiên bản cuối)					
	- Cách viết tài liệu hướng dẫn sử dụng và về các đề mục cần mô tả. - Tiến trình rà soát. - Công việc của người sử dụng. - Vận hành hệ thống. - Thiết kế giao diện đồ họa cho người sử dụng (GUI) và thực hiện.	- Lựa chọn phương pháp trao đổi phù hợp cho việc rà soát tài liệu hướng dẫn người sử dụng và thực hiện việc rà soát một cách hiệu quả. - Trình bày giao diện đồ họa người sử dụng (GUI) thông qua thiết kế chi tiết và tiếp nhận hiểu biết của những người tham gia trong quá trình rà soát. - Sắp xếp các yêu cầu vận hành một cách hệ thống.				
SDSS 6	**Mô đun: Xây dựng chương trình**		**x**	**x**	**x**	**x**
SDSS 6.1	Lập trình (Coding)					
	- Phương pháp luận về sự phát triển của lập trình. - Lập trình SQL. - Chất lượng chương trình (ví dụ: sự thuận tiện trong việc đọc chương trình (decoding), bảo trì, hiệu quả). - Ngôn ngữ lập trình thích hợp với việc phát triển ứng dụng.	- Xác định rõ các tài liệu hướng dẫn lập trình và cân nhắc các đặc tả chi tiết. - Tóm tắt các thông tin xử lý. - Tạo các mã nguồn khác nhau đối với các vấn đề phức tạp để có thể so sánh, đánh giá. - Tìm hiểu kiến trúc và phân cấp trong hệ thống.				

Mã tham chiếu	Nội dung/ Yêu cầu cần đạt		Yêu cầu cần đạt theo hạng			
	Kiến thức	Kỹ năng	4	3	2	1
	- Việc sử dụng lại các thành phần đã có.	- Đảm bảo chất lượng phần mềm theo yêu cầu. - Xây dựng cấu trúc chương trình có tính mở rộng, linh hoạt và tin cậy.				
SDSS 6.2	Rà soát mã nguồn bởi đồng nghiệp (peer-review code)					
	- Kỹ thuật và trình tự rà soát mã nguồn bởi đồng nghiệp.	- Lựa chọn nhóm tham gia rà soát thích hợp. - Lựa chọn phương pháp trao đổi phù hợp và thực hiện việc rà soát. - So sánh các cách lập trình dựa trên các kỹ thuật lập trình khác nhau. - Giải thích các vấn đề có tính logic và dữ liệu phức tạp. - Mô phỏng mã nguồn và phân tích kết quả. - Đánh giá đúng các ý kiến phản biện.				
SDSS 6.3	Kiểm thử đơn vị					
	- Thủ tục kiểm thử đơn vị. - Quy trình kiểm thử lặp. - Phương pháp phân tích lỗi và quy trình sửa lỗi.	- Xác định, xử lý và hiệu chỉnh các sai sót và lỗi. - Kiểm tra, phân tích trạng thái và đề xuất giải pháp.				
SDSS 6.4	Kiểm thử thành phần					
	- Thủ tục kiểm thử thành phần. - Quy trình kiểm thử lặp. - Phương pháp phân tích lỗi và quy trình sửa lỗi. - Kiểm tra tính chính xác của phần mềm.	- Xác định, xử lý và hiệu chỉnh các sai sót và lỗi. - Kiểm tra, phân tích trạng thái và đề xuất giải pháp. - Kiểm tra tính chính xác của phần mềm.				
SDSS 6.5	Kiểm thử hệ thống					
	- Thủ tục kiểm thử hệ thống. - Quy trình kiểm thử lặp. - Phương pháp phân tích lỗi và quy trình sửa lỗi. - Kiểm tra tính chính xác của hệ thống.	- Xác định, xử lý và hiệu chỉnh các sai sót và lỗi. - Kiểm tra, phân tích trạng thái và đề xuất giải pháp. - Tìm hiểu kiến trúc và phân cấp của hệ thống. - Phân loại quá trình và kết quả một cách hệ thống và viết thành văn bản làm tài liệu minh chứng chi tiết.				
SDSS 6.6	Kiểm thử yêu cầu hệ thống hóa					

Mã tham chiếu	Nội dung/ Yêu cầu cần đạt		Yêu cầu cần đạt theo hạng			
	Kiến thức	Kỹ năng	4	3	2	1
	- Thủ tục kiểm thử yêu cầu hệ thống hóa. - Quy trình kiểm thử lặp. - Phương pháp phân tích lỗi và quy trình sửa lỗi.	- Xác định, giải quyết và hiệu chỉnh các sai sót và lỗi. - Phát hiện, phân tích trạng thái và đề xuất giải pháp. - Tìm hiểu kiến trúc và phân cấp của hệ thống. - Phân loại quá trình và kết quả một cách hệ thống và viết thành văn bản làm tài liệu minh chứng chi tiết. - Chuẩn bị các phương án khác nhau và đàm phán với người sử dụng nếu yêu cầu của người sử dụng không được thỏa mãn do sai sót kỹ thuật hoặc hệ thống.				
SDSS 6.7	Cập nhật tài liệu					
	- Xây dựng tài liệu hướng dẫn sử dụng. - Xây dựng tài liệu hệ thống. - Quy trình cập nhật tài liệu. - Vận hành hệ thống.	- Giải thích về các thay đổi trong tài liệu hướng dẫn sử dụng và nguyên nhân. - Phản ánh sự thay đổi trong thiết kế hệ thống hoặc trong thực hiện ở tài liệu hệ thống.				
SDSS 6.8	Chuẩn bị bàn giao phần mềm					
	- Cấu hình sản phẩm phần mềm để bàn giao. - Các thủ tục chuẩn bị bàn giao. - Bàn giao sản phẩm để đưa vào vận hành và các giai đoạn bảo trì	- Tổ chức, sắp xếp phần mềm, dữ liệu, tài liệu liên quan theo mẫu bàn giao. - Giải thích các mục liên quan đến việc bàn giao phần mềm.				
SDSS 7	**Mô đun: Hỗ trợ cài đặt phần mềm**		**x**	**x**	**x**	**x**
SDSS 7.1	Cài đặt phần mềm					
	- Hệ thống hiện tại của người sử dụng. - Cài đặt phần mềm. - Việc vận hành song song với hệ thống hiện tại.	- Lập kế hoạch cài đặt phần mềm ít ảnh hưởng nhất đến môi trường hiện tại của người sử dụng. - Hỗ trợ người sử dụng từ giai đoạn vận hành đầu tiên.				
SDSS 7.2	Hỗ trợ kiểm thử chấp nhận của người sử dụng					
	- Hiểu về các kết quả kiểm thử hệ thống và kết quả kiểm thử yêu cầu hệ thống hóa	- Thực hiện các công việc hỗ trợ cho quá trình kiểm thử chấp nhận theo yêu cầu của người sử dụng				
SDSS 7.3	Đào tạo, huấn luyện và hỗ trợ người sử dụng					
	- Việc vận hành phần mềm của người sử dụng.	- Lập kế hoạch đào tạo, huấn luyện và hỗ trợ phù hợp với năng lực của người sử dụng phần mềm.				

Mã tham chiếu	Nội dung/ Yêu cầu cần đạt		Yêu cầu cần đạt theo hạng			
	Kiến thức	Kỹ năng	4	3	2	1
		- Đào tạo, huấn luyện và hỗ trợ người sử dụng.				
SDSS 8	**Mô đun: Các hoạt động kiểm thử chung**		**x**	**x**	**x**	**x**
SDSS 8.1	Chuẩn bị kế hoạch kiểm thử					
	- Bảo đảm chất lượng phần mềm. - Tính tin cậy của phần mềm. - Lịch kiểm thử. - Tổ chức các hệ thống kiểm thử. - Kỹ thuật kiểm thử. - Thiết kế và chuẩn bị dữ liệu kiểm thử. - Phương pháp đánh giá kết quả kiểm thử. - Các tài liệu kết quả kiểm thử. - Chuẩn bị môi trường kiểm thử. - Công cụ và phương tiện kiểm thử	- Lập kế hoạch bảo đảm chất lượng trong quy trình phát triển hệ thống. - Chuẩn bị lịch trình kiểm thử hợp lý. - Đánh giá các tài nguyên và nhân lực cần để thực hiện kiểm thử. - Lựa chọn phương pháp kiểm thử phù hợp với dự án. - Nghiên cứu tự động hóa quy trình kiểm thử. - Xác định điều kiện bắt đầu và kết thúc kiểm thử.				
SDSS 8.2	Chuẩn bị quy trình kiểm thử					
	- Phương pháp luận kiểm thử	- Giám sát thủ tục kiểm thử				
SDSS 8.3	Thực hiện kiểm thử					
	- Quy trình kiểm thử. - Phương pháp luận kiểm thử. - Quy trình kiểm thử lặp. - Phân tích lỗi và sửa lỗi. - Báo cáo kết quả kiểm thử.	- Đánh giá kết quả kiểm thử. - Xác định, giải quyết và hiệu chỉnh các sai sót và lỗi. - Kiểm tra, phân tích trạng thái và đề xuất giải pháp. - Phân loại các quy trình, kết quả một cách hệ thống và lập tài liệu. - Đánh giá hiệu năng. - Đánh giá tính khả dụng. - Đánh giá các thủ tục kiểm thử.				
SDSS 8.4	Ghi nhận kết quả kiểm thử và phê duyệt					
	- Các tài liệu ghi nhận kết quả kiểm thử.	- Đánh giá các công cụ kiểm thử tự động. - Đánh giá tính đầy đủ của kiểm thử. - Nghiên cứu kế hoạch cải tiến thủ tục kiểm thử.				