Ký bởi: CÔNG BÁO NƯỚC CỘNG HÒA XÃ HỘI CHỦ NGHĨA VIỆT NAM
Cơ quan: VĂN PHÒNG CHÍNH PHỦ
Ngày ký: 2026-10-22 16:12:36 +07:00

THỦ TƯỚNG CHÍNH PHỦ

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

Số: 1964/QĐ-TTg

Hà Nội, ngày 12 tháng 10 năm 2026

QUYẾT ĐỊNH
Về việc ban hành Chỉ số bảo đảm an ninh mạng

THỦ TƯỚNG CHÍNH PHỦ

Căn cứ Luật Tổ chức Chính phủ ngày 18 tháng 02 năm 2025;

Căn cứ Luật An ninh mạng ngày 10 tháng 12 năm 2025;

Căn cứ Luật Bảo vệ bí mật nhà nước ngày 10 tháng 12 năm 2025;

Căn cứ Chỉ thị số 57-CT/TW, ngày 31/12/2025 của Ban Bí thư về tăng cường bảo đảm an ninh mạng, bảo mật thông tin, an ninh dữ liệu trong hệ thống chính trị;

Theo đề nghị của Bộ trưởng Bộ Công an.

QUYẾT ĐỊNH:

Điều 1. Phê duyệt ban hành và triển khai Chỉ số bảo đảm an ninh mạng (sau đây viết gọn là Chỉ số) giai đoạn 2027 - 2028, định hướng đến năm 2030 như sau:

1. Giai đoạn 2027 - 2028: Triển khai thử nghiệm, đánh giá, cập nhật, điều chỉnh Chỉ số gồm 03 nhóm tiêu chí với 29 tiêu chí thành phần. Nội dung chi tiết, nguyên tắc, cấu trúc chỉ số, quy trình tính toán, thang đánh giá của Chỉ số được thực hiện dựa trên 07 Phụ lục kèm theo Quyết định này. Trong quá trình triển khai thử nghiệm, các nội dung quy định tại Phụ lục được cập nhật, hiệu chỉnh nhằm bảo đảm tính khả thi và phù hợp với thực tiễn trước khi áp dụng chính thức. Việc sơ kết giai đoạn triển khai thử nghiệm được thực hiện trong Quý II năm 2028. Kết quả đánh giá trong giai đoạn triển khai thử nghiệm này được cơ quan thường trực sử dụng làm cơ sở thực tiễn để rà soát, hoàn thiện Chỉ số, không tổng hợp làm căn cứ xét thi đua, khen thưởng hoặc đánh giá mức độ hoàn thành nhiệm vụ của các bộ, cơ quan ngang bộ, Ủy ban nhân dân cấp tỉnh (sau đây gọi là các bộ, cơ quan, địa phương).

2. Trên cơ sở kết quả sơ kết giai đoạn triển khai thử nghiệm quy định tại khoản 1 Điều này, cơ quan thường trực báo cáo, đề xuất Thủ tướng Chính phủ xem xét, quyết định việc áp dụng chính thức Chỉ số cho giai đoạn 2029 - 2030 và định hướng các năm tiếp theo, bảo đảm phù hợp với xu hướng công nghệ mới và yêu cầu quản trị an ninh mạng quốc gia.

Điều 2. Phạm vi triển khai thí điểm

1. Trong giai đoạn 2027 - 2028 quy định tại Điều 1 Quyết định này, các bộ, cơ quan, địa phương tổ chức đánh giá thí điểm Chỉ số trên cơ sở áp dụng cấu trúc, nguyên tắc và phương pháp của Chỉ số nêu tại các Phụ lục kèm theo Quyết định này. Cơ quan, tổ chức khác có nhu cầu có thể nghiên cứu, tham khảo để tự tổ chức đánh giá. Hồ sơ đề xuất cấp độ hệ thống thông tin đã được phê duyệt trước ngày Quyết định này có hiệu lực thi hành tiếp tục được sử dụng làm căn cứ đánh giá Chỉ số cho đến khi được rà soát, điều chỉnh hoặc phê duyệt lại theo quy định.

2. Việc đánh giá Chỉ số trong giai đoạn thí điểm được thực hiện theo hướng dẫn của cơ quan thường trực quy định tại Điều 4 Quyết định này, trên cơ sở số liệu, kết quả triển khai thực tế và hồ sơ, tài liệu minh chứng của kỳ đánh giá tương ứng.

Điều 3. Xử lý kết quả đánh giá

1. Kết quả đánh giá Chỉ số được bảo mật, quản lý, sử dụng theo quy định; bảo đảm tuân thủ quy định pháp luật về bảo vệ bí mật nhà nước đối với các nội dung có chứa bí mật nhà nước. Trường hợp công bố theo quy định tại khoản 3 Điều này, nội dung công bố gồm điểm số và mức xếp loại của cơ quan, tổ chức.

2. Đối với kết quả đánh giá thử nghiệm (giai đoạn 2027 - 2028): Kết quả giai đoạn này là cơ sở thực tiễn để rà soát, hoàn thiện cấu trúc, tiêu chí và phương pháp tính toán của Chỉ số.

3. Đối với kết quả đánh giá chính thức (từ năm 2029 trở đi): Kết quả đánh giá được tổng hợp, báo cáo Thủ tướng Chính phủ và tổ chức công bố, xếp hạng định kỳ theo quy định trước tháng 5 hằng năm; làm căn cứ quan trọng trong công tác quản lý nhà nước, phục vụ hoạch định chính sách vĩ mô, chiến lược về an ninh mạng quốc gia. Kết quả đánh giá chính thức có thể được sử dụng làm một trong các thông tin tham khảo phục vụ công tác đánh giá cán bộ, công chức theo quy định của pháp luật về cán bộ, công chức và quy định khác có liên quan.

Điều 4. Tổ chức thực hiện

1. Bộ Công an là cơ quan thường trực theo dõi, đánh giá, tổng hợp kết quả đánh giá Chỉ số hằng năm; chủ trì, phối hợp Bộ Khoa học và Công nghệ, Bộ Quốc phòng và các bộ, cơ quan, địa phương đề xuất điều chỉnh Chỉ số; sơ kết, tổng kết việc triển khai thử nghiệm; xem xét, điều chỉnh đối với các nhóm tiêu chí, tiêu chí thành phần để phù hợp với tình hình thực tiễn; hướng dẫn việc áp dụng Chỉ số, phương pháp đánh giá, phạm vi và thời điểm thu thập dữ liệu đánh giá, việc áp dụng các tiêu chuẩn, quy chuẩn kỹ thuật và các vấn đề phát sinh trong quá trình triển khai thực hiện Chỉ số; nghiên cứu, xây dựng công cụ hỗ trợ đánh giá tự động, xây dựng hệ thống thông tin phục vụ việc chấm điểm, tổng hợp, báo cáo, thống kê kết quả đánh giá hằng năm.

2. Các bộ, cơ quan, địa phương tổ chức đánh giá đối với các hệ thống thông tin thuộc phạm vi quản lý, bao gồm hệ thống thông tin của các đơn vị trực thuộc; xây dựng cơ chế, chính sách phù hợp để theo dõi, thống kê, tổng hợp số liệu các chỉ tiêu, đảm bảo cập nhật thường xuyên, liên tục, đầy đủ, chính xác và báo cáo về cơ quan thường trực để tổng hợp, đánh giá theo thời hạn do cơ quan thường trực hướng dẫn; tăng cường ứng dụng khoa học, công nghệ để hình thành hệ thống dữ liệu đầy đủ, hỗ trợ cho việc triển khai đánh giá Chỉ số.

3. Công an tỉnh, thành phố là đầu mối tham mưu cho Ủy ban nhân dân tỉnh, thành phố tổ chức triển khai thực hiện Quyết định này; phối hợp với các cơ quan, tổ chức có liên quan trong việc theo dõi, tổng hợp, báo cáo kết quả đánh giá theo quy định.

Điều 5. Quyết định này có hiệu lực thi hành kể từ ngày ký ban hành.

Điều 6. Các Bộ trưởng, Thủ trưởng cơ quan ngang bộ, Chủ tịch Ủy ban nhân dân các tỉnh, thành phố và các tổ chức, cá nhân có liên quan chịu trách nhiệm thi hành Quyết định này./.

KT. THỦ TƯỚNG
PHÓ THỦ TƯỚNG

Phạm Gia Túc

Phụ lục I

NHỮNG VẤN ĐỀ CHUNG VÀ CẤU TRÚC TỔNG THỂ CHỈ SỐ

(Kèm theo Quyết định số 1964/QĐ-TTg ngày 12 tháng 10 năm 2026 của Thủ tướng Chính phủ)

I. Ý NGHĨA, MỤC ĐÍCH, YÊU CẦU

1. Ý nghĩa

Chỉ số được xây dựng nhằm đánh giá một cách thống nhất, khách quan và định lượng mức độ bảo đảm an ninh mạng của các bộ, cơ quan, địa phương làm cơ sở theo dõi, so sánh, xếp hạng kết quả thực hiện, kịp thời phát hiện các tồn tại, hạn chế và nguy cơ mất an ninh mạng, đồng thời phục vụ công tác quản lý nhà nước, kiểm tra, giám sát, hoạch định chính sách bảo đảm an ninh mạng.

2. Mục đích

Chỉ số có ý nghĩa quan trọng trong việc nâng cao hiệu quả quản trị an ninh mạng, góp phần xây dựng môi trường số an toàn, đồng bộ và bền vững; tạo cơ sở chuẩn hóa hoạt động đánh giá, thúc đẩy các bộ, cơ quan, địa phương chủ động đầu tư nguồn lực, nâng cao năng lực phòng ngừa, phát hiện và ứng phó với các nguy cơ, sự cố an ninh mạng; đồng thời hỗ trợ cơ quan quản lý nhà nước xác định mức độ trưởng thành về an ninh mạng, ưu tiên nguồn lực và giải pháp phù hợp, nâng cao hiệu quả giám sát, điều hành và góp phần thực hiện mục tiêu bảo đảm an ninh mạng gắn với chuyển đổi số quốc gia.

3. Yêu cầu

Chỉ số cần bảo đảm tính khách quan, định lượng và khả năng đo lường; phản ánh đầy đủ năng lực thực tế về bảo đảm an ninh mạng của cơ quan, tổ chức; phù hợp với các tiêu chuẩn, quy chuẩn kỹ thuật và quy định pháp luật hiện hành; có khả năng áp dụng thống nhất trên phạm vi toàn quốc; kết hợp đánh giá các yếu tố về quản trị, kỹ thuật, tổ chức, nhân lực và ứng phó sự cố; đồng thời bảo đảm tính khả thi trong triển khai, dễ thu thập và kiểm chứng số liệu, hỗ trợ theo dõi, so sánh, đánh giá xu hướng cải thiện năng lực an ninh mạng và thúc đẩy phương thức quản trị an ninh mạng chủ động dựa trên rủi ro.

II. NGUYÊN TẮC, PHƯƠNG PHÁP XÂY DỰNG CHỈ SỐ

1. Nguyên tắc

Chỉ số được xây dựng trên cơ sở bảo đảm tính khách quan, thống nhất, minh bạch, định lượng và có khả năng đo lường được mức độ bảo đảm an ninh mạng của các bộ, cơ quan, địa phương.

Việc xây dựng và triển khai Chỉ số bám sát yêu cầu quản lý nhà nước về an ninh mạng, phù hợp với quy định pháp luật quốc gia, các tiêu chuẩn quốc gia, quy chuẩn kỹ thuật quốc gia hiện hành và định hướng chuyển đổi số quốc gia; trong đó lấy mức độ tuân thủ tiêu chuẩn TCVN 14423:2026 An ninh mạng - Hệ thống thông tin - Yêu cầu cơ bản làm cơ sở trọng tâm để đánh giá.

Chỉ số phản ánh đầy đủ các yếu tố về quản trị, kỹ thuật, vận hành, giám sát, ứng phó sự cố, bảo vệ dữ liệu, nguồn lực và trách nhiệm của người đứng đầu; bảo đảm phù hợp với đặc thù, cấp độ và phạm vi hoạt động của từng nhóm cơ quan, tổ chức, địa phương.

Việc đánh giá bảo đảm khả năng kiểm chứng, đối chiếu bằng hồ sơ, tài liệu, kết quả triển khai thực tế và dữ liệu giám sát; hạn chế đánh giá hình thức, tự khai thiếu căn cứ hoặc không phản ánh đúng thực trạng bảo đảm an ninh mạng.

Chỉ số được xây dựng theo hướng mở, bảo đảm khả năng rà soát, cập nhật, điều chỉnh định kỳ nhằm phù hợp với sự phát triển của khoa học công nghệ, tình hình an ninh mạng trong nước và quốc tế cũng như các thông lệ, khung quản trị an ninh mạng tiên tiến và các mô hình quản lý an ninh mạng.

2. Phương pháp xây dựng

Chỉ số được xây dựng theo phương pháp chấm điểm, đánh giá mức độ đáp ứng các yêu cầu, biện pháp và nhóm tiêu chí quy định trong tiêu chuẩn TCVN 14423:2026 và các quy định pháp luật có liên quan.

Cấu trúc Chỉ số được tổ chức theo các nhóm tiêu chí: mỗi tiêu chí, yêu cầu được xác định mức độ đáp ứng tương ứng với thang điểm hoặc mức đánh giá cụ thể trên cơ sở:

- Mức độ triển khai thực tế;

- Mức độ đầy đủ của hồ sơ, tài liệu, bằng chứng kiểm chứng;

- Mức độ duy trì, vận hành và hiệu quả áp dụng;

- Kết quả kiểm tra, giám sát, đánh giá độc lập hoặc dữ liệu kỹ thuật liên quan.

Kết quả đánh giá được tổng hợp theo nhóm tiêu chí và quy đổi thành mức xếp hạng nhằm phục vụ công tác theo dõi, so sánh xu hướng cải thiện năng lực bảo đảm an ninh mạng của các bộ, cơ quan, địa phương.

III. CẤU TRÚC TỔNG THỂ CỦA CHỈ SỐ VÀ QUY TRÌNH TÍNH TOÁN

1. Cấu trúc tổng thể Chỉ số

Chỉ số bao gồm 03 nhóm tiêu chí và 29 tiêu chí thành phần, cụ thể tại Phụ lục II của Quyết định này, trong đó, Nhóm I - Nhóm tiêu chí đánh giá chung và Nhóm II - Nhóm tiêu chí đánh giá đặc thù được dùng để tính toán Chỉ số, Nhóm III - Nhóm tiêu chí phục vụ chỉ đạo, điều hành không dùng để tính toán Chỉ số.

2. Quy trình tính toán Chỉ số

Quy trình tính toán Chỉ số thực hiện theo Phụ lục III, Phụ lục IV của Quyết định này.

Phụ lục II

DANH MỤC TIÊU CHÍ CỦA CHỈ SỐ

(Kèm theo Quyết định số 1964/QĐ-TTg ngày 12 tháng 10 năm 2026 của Thủ tướng Chính phủ)

STT	Tiêu chí	Trọng số[1]
I. Nhóm I - Nhóm tiêu chí đánh giá chung (áp dụng đối với mọi hệ thống thông tin, chủ quản hệ thống thông tin)		**20%**
I.1.	Đáp ứng hồ sơ đề xuất cấp độ	5
I.2.	Đáp ứng phương án bảo đảm an ninh mạng theo cấp độ	10
II. Nhóm II - Nhóm tiêu chí đánh giá đặc thù (áp dụng đối với hệ thống thông tin cấp độ 3 trở lên, chủ quản hệ thống thông tin cấp độ 3 trở lên)		**80%**
II.1.	Quản lý rủi ro an ninh mạng	10
II.2.	Quản lý tài sản phần cứng	9
II.3.	Quản lý tài sản phần mềm	9
II.4.	Quản lý tài sản thông tin	10
II.5.	Cấu hình an toàn cho phần cứng và phần mềm	10
II.6.	Quản lý tài khoản và quyền truy cập tài khoản của người dùng	10
II.7.	Quản lý lỗ hổng bảo mật	10
II.8.	Quản lý nhật ký an ninh mạng	9
II.9.	Bảo vệ cho trình duyệt web, dịch vụ thư điện tử	8
II.10.	Phòng chống phần mềm độc hại	9
II.11.	Sao lưu và khôi phục dữ liệu	10
II.12.	Quản lý hạ tầng mạng	9
II.13.	Giám sát phòng thủ an ninh mạng	9
II.14.	Nhân sự vận hành, quản trị hệ thống, bảo vệ an ninh mạng	8
II.15.	Quản lý nhà cung cấp sản phẩm, dịch vụ	8
II.16.	Phát triển ứng dụng an toàn	7
II.17.	Quản trị ứng phó sự cố an ninh mạng	10

[1] Trọng số là hệ số phản ánh mức độ quan trọng tương đối của từng nhóm tiêu chí, tiêu chí đối với kết quả đánh giá Chỉ số. Trọng số chỉ thể hiện mối quan hệ tương quan giữa các nhóm tiêu chí hoặc giữa các tiêu chí trong cùng một nhóm tiêu chí và không phản ánh mối quan hệ tương quan trực tiếp giữa các tiêu chí thuộc các nhóm tiêu chí khác nhau.

II.18.	Quản lý kiểm tra an ninh mạng	7
III. Nhóm III - Nhóm tiêu chí phục vụ chỉ đạo, điều hành (áp dụng đối với mọi hệ thống thông tin, chủ quản hệ thống thông tin)		**0%**
III.1.	Tỷ lệ biện pháp xử lý rủi ro được thực hiện đúng hạn theo kế hoạch (%)	
III.2.	Tỷ lệ sự cố an ninh mạng được kiểm soát và xử lý kịp thời trên tổng số lượng sự cố an ninh mạng (%)	
III.3.	Số lượng sự cố an ninh mạng nghiêm trọng xảy ra (số vụ)	
III.4.	Số bản ghi dữ liệu cá nhân của công dân bị lộ lọt (số bản ghi)	
III.5.	Số Gigabyte dữ liệu bị lộ lọt (GB)	
III.6.	Số Gigabyte dữ liệu bị mất, mã hoá (GB)	
III.7.	Số vụ lộ bí mật nhà nước trên không gian mạng do sự cố an ninh mạng gây ra (vụ)	
III.8.	Số đầu tài liệu bí mật nhà nước bị đăng tải, truyền đưa trên không gian mạng do sự cố an ninh mạng gây ra (tài liệu)	
III.9.	Thiệt hại tài chính do các sự cố an ninh mạng gây ra trên tổng ngân sách chi cho công tác bảo đảm an ninh mạng (%)	

Ý nghĩa các nhóm tiêu chí

I. Nhóm I - Nhóm tiêu chí đánh giá chung

Nhóm tiêu chí này đánh giá mức độ tuân thủ các quy định của pháp luật, hồ sơ đề xuất cấp độ và phương án bảo đảm an ninh mạng đã được phê duyệt đối với hệ thống thông tin, chủ quản hệ thống thông tin. Đây là cơ sở để bảo đảm hệ thống được triển khai, vận hành đúng quy định và đáp ứng các yêu cầu quản lý nhà nước. Tuy nhiên, nhóm tiêu chí này chủ yếu phản ánh mức độ tuân thủ cơ bản, do đó được phân bổ trọng số 15%. Các tiêu chí trong nhóm này chỉ ghi nhận đạt khi đáp ứng đầy đủ Mức 3 (không có các mức trung gian như Mức 1, Mức 2 do đây là nhóm tiêu chí đánh giá tuân thủ quy định của pháp luật); trường hợp chưa đáp ứng Mức 3 thì ghi nhận Mức 0. Nhóm I gồm có 02 tiêu chí sau:

Tiêu chí I.1. Đáp ứng hồ sơ đề xuất cấp độ

Tiêu chí này đánh giá mức độ đáp ứng của hệ thống thông tin đối với các yêu cầu đã được xác định trong hồ sơ đề xuất cấp độ. Đây là căn cứ để bảo đảm hệ thống được triển khai đúng phạm vi, chức năng và mức độ bảo vệ tương ứng với cấp độ đã được phê duyệt.

Tiêu chí I.2. Đáp ứng phương án bảo đảm an ninh mạng theo cấp độ

Tiêu chí này đánh giá việc triển khai các biện pháp bảo đảm an ninh mạng theo phương án đã được phê duyệt. Mặc dù đã có hồ sơ đề xuất cấp độ, tuy nhiên, nếu không triển khai đầy đủ các phương án bảo đảm an ninh mạng thì cũng không thể bảo vệ được hệ thống thông tin.

II. Nhóm II - Nhóm tiêu chí đánh giá đặc thù (áp dụng đối với hệ thống thông tin cấp độ 3 trở lên)

Nhóm tiêu chí này đánh giá trực tiếp năng lực quản trị, vận hành, phòng ngừa, phát hiện, ứng phó và phục hồi trước các nguy cơ, sự cố an ninh mạng đối với hệ thống thông tin cấp độ 3 trở lên, chủ quản hệ thống thông tin cấp độ 3 trở lên. Đây là nhóm phản ánh toàn diện khả năng bảo vệ hệ thống thông tin trong thực tế và có tác động trực tiếp đến việc bảo đảm tính bí mật, tính toàn vẹn và tính sẵn sàng của hệ thống. Do đóng vai trò quyết định đến hiệu quả bảo đảm an ninh mạng nên nhóm tiêu chí này được phân bổ trọng số cao nhất. Nhóm II gồm có 18 tiêu chí sau:

Tiêu chí II.1. Quản lý rủi ro an ninh mạng

Tiêu chí này đánh giá khả năng nhận diện, phân tích, đánh giá và xử lý các rủi ro có thể ảnh hưởng đến hệ thống thông tin. Đây là hoạt động mang tính định hướng cho toàn bộ công tác bảo đảm an ninh mạng, giúp tổ chức chủ động phòng ngừa các nguy cơ trước khi xảy ra sự cố.

Tiêu chí II.2. Quản lý tài sản phần cứng

Tiêu chí này đánh giá việc kiểm kê, theo dõi và quản lý các thiết bị phần cứng thuộc hệ thống thông tin. Việc quản lý đầy đủ tài sản phần cứng giúp xác định phạm vi bảo vệ và hạn chế nguy cơ phát sinh từ các thiết bị không được kiểm soát.

Tiêu chí II.3. Quản lý tài sản phần mềm

Tiêu chí này đánh giá khả năng quản lý, kiểm soát và theo dõi các phần mềm đang được sử dụng trong hệ thống. Việc kiểm soát phần mềm giúp hạn chế các phần mềm không được cấp phép hoặc tồn tại lỗ hổng bảo mật.

Tiêu chí II.4. Quản lý tài sản thông tin

Tiêu chí này đánh giá việc xác định, phân loại và quản lý các tài sản thông tin của tổ chức. Việc nhận diện chính xác giá trị và mức độ quan trọng của thông tin là cơ sở để áp dụng các biện pháp bảo vệ phù hợp; tiêu chí liên quan trực tiếp đến đối tượng cần được bảo vệ là dữ liệu.

Tiêu chí II.5. Cấu hình an toàn cho phần cứng và phần mềm

Tiêu chí này đánh giá việc thiết lập, duy trì các cấu hình bảo mật cho hệ thống. Cấu hình không an toàn là nguyên nhân phổ biến dẫn đến các sự cố an ninh mạng.

Tiêu chí II.6. Quản lý tài khoản và quyền truy cập tài khoản của người dùng

Tiêu chí này đánh giá việc kiểm soát danh tính và quyền truy cập của người sử dụng. Việc quản lý chặt chẽ tài khoản giúp ngăn ngừa truy cập trái phép và giảm thiểu nguy cơ lạm dụng quyền hạn.

Tiêu chí II.7. Quản lý lỗ hổng bảo mật

Tiêu chí này đánh giá khả năng phát hiện, đánh giá và khắc phục các lỗ hổng bảo mật tồn tại trong hệ thống. Đây là một trong những biện pháp quan trọng nhất để giảm nguy cơ bị tấn công khai thác.

Tiêu chí II.8. Quản lý nhật ký an ninh mạng

Tiêu chí này đánh giá việc thu thập, lưu trữ và phân tích các bản ghi nhật ký. Nhật ký là nguồn dữ liệu quan trọng phục vụ giám sát, điều tra và truy vết sự cố do đó, tiêu chí đóng vai trò hỗ trợ quan trọng cho công tác phát hiện và xử lý sự cố.

Tiêu chí II.9. Bảo vệ cho trình duyệt web, dịch vụ thư điện tử

Tiêu chí này đánh giá việc triển khai các biện pháp bảo vệ đối với các kênh giao tiếp phổ biến của người dùng. Đây là các mục tiêu thường xuyên bị lợi dụng để phát tán mã độc hoặc thực hiện tấn công lừa đảo.

Tiêu chí II.10. Phòng chống phần mềm độc hại

Tiêu chí này đánh giá khả năng phát hiện, ngăn chặn và xử lý các phần mềm độc hại. Đây là lớp bảo vệ cơ bản nhưng rất quan trọng đối với mọi hệ thống thông tin, có ảnh hưởng trực tiếp đến khả năng bảo vệ thiết bị đầu cuối và máy chủ hệ thống.

Tiêu chí II.11. Sao lưu và khôi phục dữ liệu

Tiêu chí này đánh giá khả năng bảo đảm dữ liệu có thể được phục hồi khi xảy ra sự cố hoặc thảm họa. Đây là biện pháp trọng yếu để duy trì hoạt động liên tục của hệ thống và giảm thiểu thiệt hại khi bị tấn công.

Tiêu chí II.12. Quản lý hạ tầng mạng

Tiêu chí này đánh giá khả năng quản lý và bảo vệ các thành phần hạ tầng mạng. Hạ tầng mạng là môi trường kết nối toàn bộ các thành phần của hệ thống thông tin và có vai trò quan trọng đối với an toàn và ổn định của hệ thống.

Tiêu chí II.13. Giám sát phòng thủ an ninh mạng

Tiêu chí này đánh giá khả năng theo dõi, phát hiện và cảnh báo các hành vi bất thường hoặc dấu hiệu tấn công. Công tác giám sát giúp rút ngắn thời gian phát hiện và xử lý sự cố, đóng vai trò quan trọng trong năng lực phòng thủ chủ động.

Tiêu chí II.14. Nhân sự vận hành, quản trị hệ thống, bảo vệ an ninh mạng

Tiêu chí này đánh giá năng lực, trách nhiệm và sự sẵn sàng của đội ngũ nhân sự. Con người là yếu tố quyết định hiệu quả thực hiện các biện pháp kỹ thuật và quản lý do đó tiêu chí mang tính hỗ trợ cho toàn bộ hoạt động bảo đảm an ninh mạng.

Tiêu chí II.15. Quản lý nhà cung cấp sản phẩm, dịch vụ

Tiêu chí này đánh giá khả năng kiểm soát các rủi ro phát sinh từ bên thứ ba. Việc quản lý nhà cung cấp giúp hạn chế các nguy cơ từ chuỗi cung ứng và các dịch vụ thuê ngoài.

Tiêu chí II.16. Phát triển ứng dụng an toàn

Tiêu chí này đánh giá việc tích hợp các yêu cầu an toàn thông tin trong quá trình phát triển phần mềm. Việc bảo đảm an toàn ngay từ giai đoạn thiết kế giúp giảm thiểu lỗ hổng phát sinh sau này, tuy nhiên, tiêu chí chỉ áp dụng đối với các hệ thống có hoạt động phát triển phần mềm.

Tiêu chí II.17. Quản trị ứng phó sự cố an ninh mạng

Tiêu chí này đánh giá khả năng chuẩn bị, tổ chức và thực hiện các hoạt động ứng phó sự cố. Năng lực ứng phó quyết định trực tiếp đến khả năng giảm thiểu tác động và phục hồi sau sự cố.

Tiêu chí II.18. Quản lý kiểm tra an ninh mạng

Tiêu chí này đánh giá việc thực hiện các hoạt động kiểm tra, đánh giá và rà soát định kỳ đối với hệ thống thông tin. Hoạt động kiểm tra giúp phát hiện các điểm yếu và nâng cao hiệu quả bảo vệ hệ thống.

III. Nhóm III - Nhóm tiêu chí phục vụ chỉ đạo, điều hành

Nhóm tiêu chí này đánh giá hiệu quả thực tế của công tác bảo đảm an ninh mạng thông qua các chỉ số phản ánh tình hình xử lý rủi ro, kiểm soát sự cố, mức độ thiệt hại và khả năng bảo vệ dữ liệu đối với hệ thống thông tin, chủ quản hệ thống thông tin. Đây là nhóm tiêu chí phản ánh trực tiếp kết quả đầu ra của toàn bộ hoạt động quản trị và bảo vệ an ninh mạng, tuy nhiên, kết quả có thể chịu tác động của nhiều yếu tố khách quan, do đó, Nhóm III chỉ phục vụ công tác chỉ đạo, điều hành, không sử dụng để tính toán chỉ số, gồm có 09 tiêu chí sau:

Tiêu chí III.1. Tỷ lệ biện pháp xử lý rủi ro được thực hiện đúng hạn theo kế hoạch (%)

Tiêu chí này đánh giá mức độ thực hiện các biện pháp xử lý rủi ro đã được phê duyệt. Việc triển khai đúng tiến độ thể hiện khả năng kiểm soát rủi ro một cách chủ động và có hệ thống, góp phần giảm thiểu khả năng xảy ra sự cố an ninh mạng hoặc giảm thiểu thiệt hại do sự cố gây ra.

Tiêu chí III.2. Tỷ lệ sự cố an ninh mạng được kiểm soát và xử lý kịp thời trên tổng số lượng sự cố an ninh mạng (%)

Tiêu chí này đánh giá hiệu quả của hoạt động phát hiện và ứng phó sự cố. Tỷ lệ xử lý kịp thời càng cao cho thấy năng lực vận hành và bảo vệ hệ thống càng hiệu quả.

Tiêu chí III.3. Số lượng sự cố an ninh mạng nghiêm trọng xảy ra (số vụ)

Tiêu chí này phản ánh khả năng xử lý sự cố thực tế của hệ thống thông tin thông qua số lượng sự cố nghiêm trọng phát sinh. Đây là chỉ số phản ánh trực tiếp hiệu quả của các biện pháp bảo vệ đã triển khai.

Tiêu chí III.4. Số bản ghi dữ liệu cá nhân của công dân bị lộ lọt (số bản ghi)

Tiêu chí này đánh giá hiệu quả bảo vệ dữ liệu cá nhân trong hệ thống thông tin. Việc để xảy ra lộ lọt dữ liệu cá nhân có thể ảnh hưởng đến quyền và lợi ích hợp pháp của công dân; tiêu chí phản ánh một trong số các yếu tố về thiệt hại do các sự cố an ninh mạng gây ra.

Tiêu chí III.5. Số Gigabyte dữ liệu bị lộ lọt (GB)

Tiêu chí này đánh giá quy mô dữ liệu bị ảnh hưởng trong các sự cố rò rỉ dữ liệu. Khối lượng dữ liệu bị lộ lọt càng lớn thì mức độ ảnh hưởng đến tổ chức càng nghiêm trọng; tiêu chí phản ánh một trong số các yếu tố về thiệt hại do các sự cố an ninh mạng gây ra.

Tiêu chí III.6. Số Gigabyte dữ liệu bị mất, mã hoá (GB)pp

Tiêu chí này đánh giá mức độ ảnh hưởng đến tính sẵn sàng và khả năng sử dụng dữ liệu. Đây là hậu quả thường gặp trong các cuộc tấn công mã độc tống tiền hoặc sự cố vận hành; tiêu chí phản ánh một trong số các yếu tố về thiệt hại do các sự cố an ninh mạng gây ra.

Tiêu chí III.7. Số vụ lộ bí mật nhà nước trên không gian mạng do sự cố an ninh mạng gây ra (vụ)

Tiêu chí này đánh giá hiệu quả bảo vệ thông tin thuộc phạm vi bí mật nhà nước. Việc để xảy ra lộ bí mật nhà nước có thể gây hậu quả đặc biệt nghiêm trọng đối với lợi ích quốc gia và cơ quan quản lý; tiêu chí phản ánh một trong số các yếu tố về thiệt hại do các sự cố an ninh mạng gây ra.

Tiêu chí III.8. Số đầu tài liệu bí mật nhà nước bị đăng tải, truyền đưa trên không gian mạng do sự cố an ninh mạng gây ra (tài liệu)

Tiêu chí này đánh giá quy mô và mức độ ảnh hưởng của các sự cố liên quan đến bí mật nhà nước. Đây là chỉ số cụ thể hóa hậu quả của việc mất an toàn đối với các tài liệu mật; tiêu chí phản ánh một trong số các yếu tố về thiệt hại do các sự cố an ninh mạng gây ra.

Tiêu chí III.9. Thiệt hại tài chính do các sự cố an ninh mạng gây ra trên tổng ngân sách chi cho công tác bảo đảm an ninh mạng (%)

Tiêu chí này đánh giá tác động kinh tế của các sự cố an ninh mạng đối với tổ chức. Đây là chỉ số tổng hợp phản ánh hậu quả cuối cùng của các rủi ro và sự cố phát sinh; tiêu chí phản ánh một trong số các yếu tố về thiệt hại do các sự cố an ninh mạng gây ra.

Phụ lục III

PHƯƠNG PHÁP ĐÁNH GIÁ ĐỐI VỚI HỆ THỐNG THÔNG TIN

(Kèm theo Quyết định số 1964/QĐ-TTg ngày 12 tháng 10 năm 2026 của Thủ tướng Chính phủ)

Bước 1: Xác định cấp độ của hệ thống thông tin

Nguyên tắc: tuân thủ quy định của pháp luật về an ninh mạng, bao gồm Luật An ninh mạng năm 2025 và các văn bản quy định chi tiết, hướng dẫn thi hành.

Căn cứ theo Luật An ninh mạng năm 2025, Nghị định số 331/2026/NĐ-CP ngày 19/8/2026 của Chính phủ về bảo vệ an ninh mạng đối với hệ thống thông tin và các văn bản quy định chi tiết, hướng dẫn thi hành, thực hiện xác định cấp độ của hệ thống thông tin cần đánh giá.

Bước 2: Tổng hợp, đánh giá và chấm điểm cho các tiêu chí đánh giá tại Phụ lục V, VI, VII

Nguyên tắc đánh giá, chấm điểm:

Nội dung, Mức đánh giá tại các Phụ lục III, IV, V, VI là thang tự đánh giá phục vụ giai đoạn triển khai thử nghiệm, không phải là quy chuẩn, tiêu chuẩn kỹ thuật bắt buộc áp dụng chung. Chủ quản hệ thống thông tin tự đánh giá và chấm điểm cho các tiêu chí, mục tiêu đánh giá theo từng nội dung đánh giá với nguyên tắc sau:

- Đánh giá và cho điểm các *nội dung đánh giá* từ Mức 0 đến Mức 3, lấy điểm số theo Mức cao nhất mà hệ thống thông tin đáp ứng. Ví dụ: hệ thống thông tin có *nội dung đánh giá II.1.1.1. Thực hiện phân tích, đánh giá rủi ro an ninh mạng* đáp ứng Mức 3 (đã đáp ứng Mức 1 và Mức 2) thì được tính 03 điểm cho nội dung đánh giá này.

- Để nội dung đánh giá được ghi nhận đạt các Mức tương ứng (Mức 1, Mức 2, Mức 3), cần có thuyết minh về thực trạng đáp ứng và các tài liệu, bằng chứng chứng minh kèm theo. Trường hợp không có thuyết minh hoặc không có tài liệu, bằng chứng chứng minh cho thuyết minh thuộc Mức nào thì không ghi nhận đạt Mức đó.

- Đối với Mức 1, trường hợp nội dung đánh giá yêu cầu có quy trình, quy định thì quy trình, quy định đó cần được ký bởi cấp có thẩm quyền và còn hiệu lực.

- Đối với Mức 2, cần có các chỉ số đo lường hiệu quả, hiệu suất thực hiện hoạt động; có cơ chế thu thập, lưu trữ, cập nhật và theo dõi số liệu; đã thực hiện đánh giá định kỳ trên cơ sở các số liệu đã thu thập để xác định mức độ hoàn thành mục tiêu, hiệu quả của hoạt động và làm căn cứ cải tiến, khắc phục các tồn tại (nếu có). Hệ thống hoặc phần mềm quản lý có khả năng lưu trữ, thống kê và truy xuất các số liệu phục vụ đánh giá.

- Đối với Mức 3, đã sử dụng kết quả đo lường, đánh giá để xác định các tồn tại, nguyên nhân và cơ hội cải tiến; đã xây dựng, triển khai các biện pháp cải tiến đối với quy trình và hoạt động có liên quan; có báo cáo đánh giá, đề xuất và theo dõi việc thực hiện các biện pháp cải tiến trên cơ sở dữ liệu, số liệu đo lường được cập nhật định kỳ.

- Đối với các nội dung không áp dụng cho hệ thống thông tin, không thực hiện chấm điểm đối với nội dung đó nếu cơ quan, tổ chức có thuyết minh rõ ràng về phạm vi loại trừ và cung cấp tài liệu, bằng chứng chứng minh không áp dụng. Bằng chứng có thể bao gồm nhưng không giới hạn ở: tài liệu mô tả phạm vi, kiến trúc hệ thống, danh mục tài sản công nghệ thông tin, cấu hình hệ thống, quy trình vận hành, văn bản quy định nội bộ hoặc tài liệu kỹ thuật liên quan chứng minh hệ thống không có đối tượng, chức năng hoặc điều kiện kỹ thuật thuộc phạm vi của tiêu chí đánh giá. Trường hợp chưa có thuyết minh hoặc tài liệu, bằng chứng nêu trên tại thời điểm đánh giá, nội dung đánh giá tương ứng được tạm ghi nhận ở Mức 0 cho kỳ đánh giá đó.

- Chủ quản hệ thống thông tin chịu trách nhiệm về tính xác thực của văn bản, tài liệu hoặc bằng chứng chứng minh được đưa ra để làm căn cứ.

- Trường hợp chủ quản hệ thống thông tin không trực tiếp quản trị, vận hành, bảo đảm an ninh mạng cho hệ thống thông tin thì đề nghị đơn vị quản trị, vận hành, bảo đảm an ninh mạng phối hợp đánh giá; đơn vị quản trị, vận hành, bảo đảm an ninh mạng tuân thủ các quy định, quy trình của chủ quản hệ thống thông tin trong quá trình phối hợp đánh giá.

- Đối với hệ thống thông tin sử dụng dịch vụ điện toán đám mây, trường hợp nhà cung cấp dịch vụ không cung cấp được tài liệu minh chứng đáp ứng các mức của nội dung đánh giá nhưng có chứng nhận đáp ứng tiêu chuẩn khác bao hàm nội dung đó thì được đánh giá đạt mức tương ứng.

- Đối với hệ thống thông tin triển khai trên hạ tầng dùng chung, đơn vị quản lý, vận hành hạ tầng chịu trách nhiệm đánh giá các tiêu chí thuộc phạm vi hạ tầng dùng chung; đơn vị quản lý, vận hành hệ thống thông tin chịu trách nhiệm đánh giá các tiêu chí còn lại thuộc phạm vi quản lý; chủ quản hệ thống thông tin chịu trách nhiệm tổng hợp kết quả đánh giá và báo cáo theo quy định.

Quá trình thực hiện:

- Đánh giá và chấm điểm cho các nội dung đánh giá *(cột 3)* thuộc *nhóm tiêu chí đánh giá chung (Nhóm I)* trong bảng tại Phụ lục V; đánh giá từ Mức 0 đến Mức 3. Điểm của *nội dung đánh giá* tương ứng với điểm của Mức đạt được.

- Đối với **hệ thống thông tin cấp độ 3 trở lên**, thực hiện đánh giá bổ sung cho các *nội dung đánh giá* thuộc *nhóm tiêu chí đánh giá đặc thù (Nhóm II)* trong bảng tại Phụ lục VI; đánh giá từ Mức 0 đến Mức 3. Điểm của *nội dung đánh giá* tương ứng với số Mức đạt được.

- Thu thập, tổng hợp số liệu các tiêu chí thuộc *Nhóm III* theo hướng dẫn tại Phụ lục VII để phục vụ công tác chỉ đạo, điều hành.

Bước 3: Tổng hợp điểm số

Bước 3.1: Tổng hợp điểm số của *Nhóm I* tại Phụ lục V

- Tổng hợp điểm số của từng *mục tiêu đánh giá (cột 2)* theo điểm của *nội dung đánh giá (đã tính ở Bước 2)* bằng cách tính bình quân cộng của điểm số các *nội dung đánh giá* cần tính điểm, cụ thể:

$$X_{Iij} = \frac{\sum_{k=1}^{n} x_{Iijk}}{n'}$$

Trong đó:

X_{Iij} là điểm số của *mục tiêu I.i.j*. Ví dụ: X_{I21} là điểm số của *mục tiêu I.2.1*,

x_{Iijk}là điểm số của *nội dung đánh giá I.i.j.k*; nếu *nội dung đánh giá* không áp dụng thì không đưa vào để tính tổng. Ví dụ: x_{I211} là điểm số của *nội dung đánh giá I.2.1.1*,

n là tổng số *nội dung đánh giá* thuộc *mục tiêu I.i.j*,

n' là số lượng *nội dung đánh giá* áp dụng thuộc *mục tiêu I.i.j* $(n' \leq n)$, không tính những *nội dung đánh giá* không áp dụng; trường hợp tất cả *nội dung đánh giá* đều không áp dụng $(n' = 0)$ thì *mục tiêu I.i.j* cũng không áp dụng để tính điểm. Ví dụ: *mục tiêu I.2.1* có 01 *nội dung đánh giá* và có 01 *nội dung đánh giá* áp dụng đối với hệ thống thông tin thì n'=1.

- Tổng hợp điểm số của từng *tiêu chí đánh giá* theo điểm của *mục tiêu đánh giá* bằng cách tính bình quân cộng của điểm số các *mục tiêu đánh giá* cần tính điểm, cụ thể:

$$X_{Ii} = \frac{\sum_{j=1}^{m} X_{Iij}}{m'}$$

Trong đó:

X_{Ii} là điểm số của *tiêu chí I.i*. Ví dụ: X_{I1} là điểm số của *tiêu chí I.1,*

X_{Iij} là điểm số của *mục tiêu đánh giá I.i.j (đã tính ở trên);* nếu *mục tiêu đánh giá* không áp dụng thì không đưa vào để tính tổng. Ví dụ: X_{I21} là điểm số của *mục tiêu đánh giá I.2.1*,

m là tổng số *mục tiêu đánh giá* thuộc *tiêu chí I.i*,

m' là số lượng *mục tiêu đánh giá* áp dụng thuộc *tiêu chí I.i* $(m' \leq m)$, không tính những *tiêu chí* không áp dụng $(m' = 0)$; trường hợp tất cả *mục tiêu đánh giá* đều không áp dụng thì *tiêu chí I.i* cũng không áp dụng để tính điểm. Ví dụ: *tiêu chí I.2* có 03 *mục tiêu đánh giá* nhưng chỉ có 02 *mục tiêu đánh giá* áp dụng đối với hệ thống thông tin thì m'=2.

- Tổng hợp điểm số của *Nhóm I* theo điểm của các *tiêu chí đánh giá* bằng cách tính bình quân cộng có trọng số điểm số của các Tiêu chí cần tính điểm, cụ thể:

$$X_I = \frac{\sum_{i=1}^{l} a_{Ii} X_{Ii}}{\sum_{i=1}^{l} a_{Ii}}$$

Trong đó:

X_I là điểm số của *Nhóm I.*

a_{Ii} là trọng số của *tiêu chí I.i* thuộc *Nhóm I*, xác định dựa theo bảng tại Phụ lục II, nếu *tiêu chí I.i* không áp dụng thì không đưa a_{Ii} vào để tính tổng,

X_{Ii} là điểm số của *tiêu chí I.i*. Ví dụ: X_{I1} là điểm số của *tiêu chí I.1*. Nếu *tiêu chí I.i* không áp dụng thì không đưa X_{Ii} vào để tính tổng,

l là tổng số lượng *tiêu chí* thuộc *Nhóm I*; trường hợp tất cả *tiêu chí* thuộc *Nhóm I* đều không áp dụng thì *Nhóm I* cũng không áp dụng để tính điểm.

Bước 3.2: Tổng hợp điểm số theo *Nhóm II* tại Phụ lục VI

- Tổng hợp điểm số của từng *mục tiêu đánh giá* theo điểm của *nội dung đánh giá* bằng cách tính bình quân cộng của điểm số các *nội dung đánh giá* cần tính điểm, cụ thể:

$$X_{IIij} = \frac{\sum_{k=1}^{n} x_{IIijk}}{n'}$$

Trong đó:

X_{IIij} là điểm số của *mục tiêu II.i.j*. Ví dụ: X_{II12} là điểm số của *mục tiêu II.1.2*,

x_{IIijk}là điểm số của *nội dung đánh giá II.i.j.k;* nếu *nội dung đánh giá* không áp dụng thì không đưa vào để tính tổng. Ví dụ: x_{II121} là điểm số của *nội dung đánh giá II.1.2.1*,

n là tổng số *nội dung đánh giá* thuộc *mục tiêu II.i.j*,

n' là số lượng *nội dung đánh giá* cần tính điểm thuộc *mục tiêu II.i.j* ($n' \leq n$), không tính những *tiêu chí* không áp dụng; trường hợp tất cả *nội dung đánh giá* đều không áp dụng ($n' = 0$) thì *mục tiêu II.i.j* cũng không áp dụng để tính điểm. Ví dụ: *mục tiêu II.1.2* có 03 *nội dung đánh giá* nhưng chỉ có 02 *nội dung đánh giá* áp dụng đối với hệ thống thông tin thì n=2.

- Tổng hợp điểm số của từng *tiêu chí* theo điểm của *mục tiêu đánh giá* bằng cách tính bình quân cộng của điểm số các *mục tiêu đánh giá* cần tính điểm, cụ thể:

$$X_{IIi} = \frac{\sum_{j=1}^{m} X_{IIij}}{m'}$$

Trong đó:

X_{IIi} là điểm số của *tiêu chí II.i*. Ví dụ: X_{II1} là điểm số của *tiêu chí II.1*,

X_{IIij} là điểm số của *mục tiêu đánh giá II.i.j*, nếu *mục tiêu đánh giá* không áp dụng thì không đưa vào để tính tổng. Ví dụ: X_{II12} là điểm số của *mục tiêu đánh giá II.1.2*,

m là tổng số *mục tiêu đánh giá* thuộc *tiêu chí II.i*,

m' là số lượng *mục tiêu đánh giá* áp dụng thuộc *tiêu chí II.i* ($m' \leq m$), không tính những *tiêu chí* không áp dụng; trường hợp tất cả *mục tiêu đánh giá* đều không áp dụng ($m' = 0$) thì *tiêu chí I.i* cũng không áp dụng để tính điểm. Ví dụ: *tiêu chí II.2* có 03 *mục tiêu đánh giá* nhưng chỉ có 02 *mục tiêu đánh giá* áp dụng đối với hệ thống thông tin thì m=2.

- Tổng hợp điểm số của *Nhóm II* theo điểm của các *tiêu chí đánh giá* bằng cách tính bình quân cộng có trọng số điểm số của các Nhóm cần tính điểm, cụ thể:

$$X_{II} = \frac{\sum_{i=1}^{l} a_{IIi} X_{IIi}}{\sum_{i=1}^{l} a_{IIi}}$$

Trong đó:

X_{II} là điểm số của Nhóm II,

a_{IIi} là trọng số của *tiêu chí II.i* thuộc *Nhóm II*, xác định dựa theo bảng tại Phụ lục II, nếu *tiêu chí II.i* không áp dụng thì không đưa a_{IIi} vào để tính tổng,

X_{IIi} là điểm số của *tiêu chí II.i.* Ví dụ: X_{II1} là điểm số của *tiêu chí II.1*. Nếu *tiêu chí II.i* không áp dụng thì không đưa X_{IIi} vào để tính tổng,

l là tổng số lượng *tiêu chí* thuộc *Nhóm II*; trường hợp tất cả *tiêu chí* thuộc *Nhóm II* đều không áp dụng thì *Nhóm II* cũng không áp dụng để tính điểm.

Bước 3.3: Tính điểm số tổng hợp

$$X_{TH} = \frac{a_I * X_I + a_{II} * X_{II}}{a_I + a_{II}}$$

Trong đó:

a_I, a_{II} là trọng số của *Nhóm I, Nhóm II;* trường hợp Nhóm không áp dụng thì trọng số của Nhóm bằng 0,

X_I, X_{II} là điểm số đánh giá của *Nhóm I, Nhóm II,*

X_{TH} là điểm số đánh giá của Hệ thống thông tin.

Bước 4: Xác định Mức trưởng thành của hệ thống thông tin

Có 04 Mức trưởng thành của hệ thống thông tin như sau:

- Mức 0 - Trạng thái phơi nhiễm: Tổ chức chưa triển khai hoặc không đáp ứng các yêu cầu tối thiểu. Ở mức độ này, hệ thống hoàn toàn phơi nhiễm trước các rủi ro và thiếu vắng sự định hướng từ ban lãnh đạo.

- Mức 1 - Trạng thái phản ứng: Tổ chức có triển khai các biện pháp ở mức cơ bản, đã thiết lập và ban hành chính thức các quy định, quy trình và có cơ chế đảm bảo tuân thủ.

- Mức 2 - Trạng thái chủ động: Tổ chức đã triển khai các biện pháp bảo mật có hệ thống, có cơ chế kiểm soát đo lường và đánh giá mức độ hiệu quả của các hoạt động. Tại mức này, an ninh mạng được quản lý bằng số liệu, cho phép phát hiện sớm sự chệch hướng trong tuân thủ và vận hành.

- Mức 3 - Trạng thái thích ứng: Biện pháp bảo vệ được triển khai chuyên sâu. Tổ chức sở hữu cơ chế cải tiến liên tục để tối ưu hóa các quy trình, chính sách, đảm bảo hệ thống có khả năng tự điều chỉnh và thích nghi trước các biến thể đe dọa mới nhất.

Tiêu chí xác định mức trưởng thành của hệ thống thông tin, tính theo mức cao nhất đạt được:

Mức đánh giá	**Điều kiện đạt**
Mức 0	Hệ thống thông tin không đạt Mức 1.
Mức 1	- Điểm tổng $X_{TH} \geq 1.4$. - Không có *tiêu chí* nào có điểm bằng 0.
Mức 2	- Hệ thống thông tin đạt Mức 1. - Điểm tổng $X_{TH} \geq 2.1$.
Mức 3	- Hệ thống thông tin đạt Mức 2. - Điểm tổng $X_{TH} \geq 2.7$. - Không có *tiêu chí* nào có điểm dưới 2.

Phụ lục IV

PHƯƠNG PHÁP ĐÁNH GIÁ ĐỐI VỚI CƠ QUAN, TỔ CHỨC

(Kèm theo Quyết định số 1964/QĐ-TTg ngày 12 tháng 10 năm 2026 của Thủ tướng Chính phủ)

Bước 1: Thu thập bảng đánh giá của từng hệ thống thông tin

Cơ quan, tổ chức thu thập bảng đánh giá của từng hệ thống thông tin của cơ quan, tổ chức, bảo đảm kết quả đánh giá chính xác, phù hợp với tiêu chí cho điểm và có đầy đủ bằng chứng chứng minh cho kết quả đánh giá.

Bước 2: Tổng hợp số liệu, điểm số đánh giá cho từng *tiêu chí đánh giá* tại Phụ lục V, VI, VII như sau:

Thống kê cấp độ của hệ thống thông tin và điểm số đạt được của từng *tiêu chí đánh giá* để tính toán điểm số tổng hợp của từng *tiêu chí*:

- Đối với *Nhóm I* và *Nhóm II (áp dụng đối với hệ thống thông tin cấp độ 3 trở lên)*, điểm số trung bình của *tiêu chí* thuộc những Nhóm này được tính theo công thức:

$$X_{TC} = \frac{\sum_{i=1}^{n} w_i X_i}{\sum_{i=1}^{n} w_i}$$

Trong đó:

n là số lượng Hệ thống thông tin của cơ quan, tổ chức; trường hợp tiêu chí không áp dụng đối với tất cả hệ thống thông tin thì tiêu chí cũng không áp dụng để tính điểm,

w_i là hệ số của hệ thống thông tin thứ i, xác định dựa trên cấp độ của Hệ thống thông tin, cụ thể:

Cấp độ Hệ thống thứ i	Cấp độ 1	Cấp độ 2	Cấp độ 3	Cấp độ 4	Cấp độ 5
w_i	1	2	3	4	5

Trường hợp tiêu chí không áp dụng đối với hệ thống thứ i thì $w_i = 0$

X_i là điểm *tiêu chí* tương ứng của Hệ thống thông tin thứ i,

X_{TC} là điểm số trung bình của *tiêu chí* cần tính điểm.

- Đối với Nhóm III, thu thập, tổng hợp số liệu thống kê thuộc *Nhóm III* theo hướng dẫn tại Phụ lục VII để phục vụ công tác chỉ đạo, điều hành. Trong đó, đối với giá trị thống kê có đơn vị là phần trăm (%), tổng hợp số liệu thống kê (không phải giá trị phần trăm) của tất cả hệ thống thông tin của cơ quan, tổ chức, sau đó mới tính giá trị thống kê phần trăm.

Bước 3: Tổng hợp điểm số đánh giá cho từng *nhóm tiêu chí* tại Phụ lục II như sau:

Điểm số trung bình của Nhóm I:

$$X_I = \frac{\sum_{i=1}^{n} a_i X_{TC\ i}}{\sum_{i=1}^{n} a_i}$$

Trong đó:

n là số lượng *tiêu chí* thuộc *Nhóm I*; trường hợp tất cả *tiêu chí* đều không áp dụng thì Nhóm I cũng không áp dụng để tính điểm,

a_i là trọng số của *tiêu chí i* thuộc *Nhóm I* áp dụng, xác định dựa theo bảng tại Phụ lục II; trường hợp *tiêu chí i* không áp dụng thì $a_i = 0$,

$X_{TC\ i}$ là điểm số trung bình của *Tiêu chí i* thuộc *Nhóm I*,

X_I là điểm số trung bình của Nhóm I,

Điểm số trung bình của Nhóm II:

$$X_{II} = \frac{\sum_{i=1}^{n} a_i X_{TC\ i}}{\sum_{i=1}^{n} a_i}$$

Trong đó:

n là số lượng *tiêu chí* thuộc *Nhóm II*; trường hợp tất cả *tiêu chí* đều không áp dụng thì *Nhóm II* cũng không áp dụng để tính điểm,

a_i là trọng số của *tiêu chí* i thuộc *Nhóm II*, xác định dựa theo bảng tại Phụ lục II, trường hợp *tiêu chí* i không áp dụng thì $a_i = 0$,

$X_{TC\ i}$ là điểm số trung bình của *tiêu chí* i thuộc *Nhóm II*,

X_{II} là điểm số trung bình của *Nhóm II*,

Bước 4: Tính hệ số quy mô hệ thống thông tin của cơ quan, tổ chức

Tính giá trị S theo công thức sau:

$$S = \sum_{i=1}^{n} w_i$$

Trong đó:

n là số lượng hệ thống thông tin của cơ quan, tổ chức,

w_i là hệ số của hệ thống thông tin thứ i, xác định dựa trên cấp độ của Hệ thống thông tin, cụ thể:

Cấp độ Hệ thống thứ i	Cấp độ 1	Cấp độ 2	Cấp độ 3	Cấp độ 4	Cấp độ 5
w_i	1	2	3	4	5

Hệ số quy mô hệ thống thông tin do cơ quan, tổ chức quản lý (K) được xác định dựa trên giá trị S theo bảng sau:

S	**S < 300**	**300 ≤ S < 500**	**S ≥ 500**
K	1.0	1.05	1.10

Bước 5: Tính điểm số tổng hợp

$$X_{TH} = K\frac{a_I * X_I + a_{II} * X_{II}}{a_I + a_{II}}$$

Trong đó:

K là hệ số quy mô hệ thống thông tin do cơ quan, tổ chức quản lý,

a_I, a_{II} là trọng số của *Nhóm I, Nhóm II;* trường hợp Nhóm không áp dụng thì trọng số của Nhóm bằng 0,

X_I, X_{II} là điểm số đánh giá của *Nhóm I, Nhóm II;*

X_{TH} là điểm số đánh giá của cơ quan, tổ chức.

Bước 6: Xác định mức xếp loại

Có 04 mức xếp loại của cơ quan, lấy mức cao nhất mà cơ quan, tổ chức đạt được, cụ thể như sau:

Mức đánh giá	**Điều kiện đạt**
Mức 0	Cơ quan, tổ chức không đạt Mức 1.
Mức 1	- Điểm tổng $X_{TH} \geq 1.4$. - Không có Hệ thống thông tin nào đạt Mức 0.
Mức 2	- Cơ quan, tổ chức đạt Mức 1. - Điểm tổng $X_{TH} \geq 2.1$.
Mức 3	- Cơ quan, tổ chức đạt Mức 2. - Điểm tổng $X_{TH} \geq 2.7$. - Không quá 10% số hệ thống ở dưới Mức 2; đối với các hệ thống này, cơ quan, tổ chức áp dụng biện pháp quản lý rủi ro phù hợp, như ngăn cách với các hệ thống khác bằng thiết bị bảo vệ an ninh mạng hoặc cô lập hoàn toàn về mặt vật lý, để hạn chế nguy cơ mất an ninh mạng đối với các hệ thống khác.

Phụ lục V

DANH MỤC ĐÁNH GIÁ THEO NHÓM TIÊU CHÍ ĐÁNH GIÁ CHUNG CHO HỆ THỐNG THÔNG TIN (NHÓM I)

(Kèm theo Quyết định số 1964/QĐ-TTg ngày 12 tháng 10 năm 2026 của Thủ tướng Chính phủ)

Tiêu chí đánh giá	Mục tiêu đánh giá	Nội dung đánh giá	Mức đánh giá				Bằng chứng
			Mức 0 (0 điểm)	Mức 1 (1 điểm)	Mức 2 (2 điểm)	Mức 3 (3 điểm)	
(1)	(2)	(3)	(4)				(5)
I.1. Đáp ứng hồ sơ đề xuất cấp độ	I.1.1. Đáp ứng hồ sơ đề xuất cấp độ	I.1.1.1. Hệ thống thông tin đã được xác định và phê duyệt cấp độ	Hệ thống thông tin chưa được xác định và phê duyệt cấp độ bởi cấp có thẩm quyền.			Hệ thống thông tin đã được xác định và phê duyệt cấp độ bởi cấp có thẩm quyền.	Hồ sơ đề xuất cấp độ đã được phê duyệt.
I.2. Đáp ứng phương án bảo đảm an ninh mạng theo cấp độ	I.2.1. Hệ thống thông tin đã triển khai đầy đủ phương án bảo đảm an ninh mạng theo cấp độ đã được phê duyệt	I.2.1.1. Hệ thống thông tin đã triển khai đầy đủ phương án bảo đảm an ninh mạng theo cấp độ đã được phê duyệt	Hệ thống thông tin chưa triển khai đầy đủ phương án bảo đảm an ninh mạng theo cấp độ đã được phê duyệt.			Hệ thống thông tin đã triển khai đầy đủ phương án bảo đảm an ninh mạng theo cấp độ đã được phê duyệt.	Thuyết minh phương án bảo đảm an ninh mạng và các tài liệu chứng minh.

Phụ lục VI

DANH MỤC ĐÁNH GIÁ THEO CÁC NHÓM TIÊU CHÍ ĐÁNH GIÁ ĐẶC THÙ CHO HỆ THỐNG THÔNG TIN (NHÓM II)

(Kèm theo Quyết định số 1964/QĐ-TTg ngày 12 tháng 10 năm 2026 của Thủ tướng Chính phủ)

Tiêu chí đánh giá	Mục tiêu đánh giá	Nội dung đánh giá	Mức đánh giá				Bằng chứng
			Mức 0 (0 điểm)	Mức 1 (1 điểm)	Mức 2 (2 điểm)	Mức 3 (3 điểm)	
(1)	(2)	(3)	(4)				(5)
II.1. Quản lý rủi ro an ninh mạng	II.1.1. Thiết lập và duy trì quy định, quy trình quản lý rủi ro an ninh mạng	II.1.1.1. Ban hành, tuân thủ quy định, quy trình quản lý rủi ro an ninh mạng	Chưa đáp ứng Mức 1.	Đã ban hành quy định, quy trình quản lý rủi ro an ninh mạng, bao gồm: xác định, phân tích, đánh giá và xử lý rủi ro an ninh mạng và có cơ chế đảm bảo tuân thủ quy định, quy trình.	Đáp ứng Mức 1 và có cơ chế đo lường, đánh giá hiệu quả thực hiện quy định, quy trình quản lý rủi ro.	Đáp ứng mức 2 và có cơ chế cải tiến liên tục để tối ưu hoá quy định, quy trình quản lý rủi ro an ninh mạng.	Quy định, quy trình quản lý rủi ro an ninh mạng, các tài liệu minh chứng.
		II.1.1.2. Đánh giá, cập nhật quy định, quy trình quản lý rủi ro an ninh mạng và các tài liệu liên quan	Chưa đáp ứng Mức 3.			Đã thực hiện việc đánh giá và cập nhật quy định, quy trình quản lý rủi ro an ninh mạng và các tài liệu liên quan tối thiểu 01 lần/năm hoặc khi có thay đổi trong tổ chức ảnh hưởng đến nội dung tài liệu.	Biên bản rà soát định kỳ, các bản cập nhật của quy định, quy trình và tài liệu liên quan, các tài liệu minh chứng.
	II.1.2. Xác định rủi ro an ninh mạng	II.1.2.1. Thực hiện xác định rủi ro an ninh mạng trong tổ chức	Chưa đáp ứng Mức 1.	Đã thực hiện xác định rủi ro an ninh mạng trong tổ chức dựa trên các hoạt động như quản lý tài sản, quản lý lỗ hổng, quản lý	Đáp ứng Mức 1 và có cơ chế đo lường, đánh giá tính hiệu quả của hoạt động	Đáp ứng Mức 2 và có cơ chế cải tiến liên tục để tối ưu hoá hoạt động xác định rủi ro an ninh mạng.	Báo cáo xác định rủi ro an ninh mạng, các tài liệu minh chứng.

				hạ tầng mạng, quản lý nhận thức an ninh mạng, quản lý tài khoản và quyền truy cập.	xác định rủi ro an ninh mạng.		
		II.1.2.2. Xác định rủi ro an ninh mạng đến từ các bên thứ ba, nhà cung cấp	Chưa đáp ứng Mức 1.	Đã thực hiện xác định rủi ro an ninh mạng đến từ các bên thứ ba, nhà cung cấp.	Đáp ứng Mức 1 và có cơ chế đo lường, đánh giá tính hiệu quả của hoạt động xác định rủi ro an ninh mạng đến từ các bên thứ ba, nhà cung cấp.	Đáp ứng Mức 2 và có cơ chế cải tiến liên tục để tối ưu hoá hoạt động xác định rủi ro an ninh mạng đến từ các bên thứ ba, nhà cung cấp.	Báo cáo xác định rủi ro an ninh mạng có xác định rủi ro từ bên thứ ba, các tài liệu minh chứng.
		II.1.2.3. Thực hiện xác định rủi ro an ninh mạng định kỳ hoặc khi có thay đổi liên quan đến hệ thống thông tin	Chưa đáp ứng Mức 3.			Đã thực hiện xác định rủi ro an ninh mạng định kỳ hoặc khi có thay đổi liên quan đến hệ thống thông tin (thay đổi hệ thống, lỗ hổng bảo mật mới, các sự kiện an ninh mạng...): - Cấp độ 3: tối thiểu 01 lần/năm; - Cấp độ 4 trở lên: tối thiểu 01 lần/06 tháng.	Báo cáo xác định rủi ro an ninh mạng định kỳ hàng năm, khi có thay đổi.
	II.1.3. Đánh giá rủi ro an ninh mạng	II.1.3.1. Thực hiện phân tích, đánh giá rủi ro an ninh mạng	Chưa đáp ứng Mức 1.	Đã thực hiện tất cả các nội dung sau: - Phân tích, đánh giá rủi ro an ninh mạng; - Xác định mức độ ảnh hưởng, tác động của rủi ro đến tổ chức; - Đưa ra quyết định chấp nhận hoặc thực hiện các biện pháp giảm thiểu rủi ro.	Đáp ứng Mức 1 và có cơ chế đo lường, đánh giá tính hiệu quả của các hoạt động sau: - Phân tích, đánh giá rủi ro an ninh mạng; - Xác định mức độ ảnh hưởng, tác động của rủi ro đến tổ chức;	Đáp ứng Mức 2 và có cơ chế cải tiến liên tục để tối ưu hoá các hoạt động sau: - Phân tích, đánh giá rủi ro an ninh mạng; - Xác định mức độ ảnh hưởng, tác động của rủi ro đến tổ chức;	Báo cáo đánh giá rủi ro an ninh mạng, các tài liệu minh chứng.

					- Đưa ra quyết định chấp nhận hoặc thực hiện các biện pháp giảm thiểu rủi ro.	- Đưa ra quyết định chấp nhận hoặc thực hiện các biện pháp giảm thiểu rủi ro.	
		II.1.3.2. Thời gian thực hiện phân tích và đánh giá rủi ro an ninh mạng	Chưa đáp ứng Mức 3.			Đã thực hiện tất cả các nội dung sau: - Phân tích, đánh giá rủi ro an ninh mạng ngay sau khi xác định rủi ro; - Phân tích, đánh giá rủi ro khi có sự thay đổi về hệ thống, các sự kiện an ninh mạng hoặc những thay đổi trong tổ chức liên quan đến rủi ro đã xác định.	Báo cáo đánh giá rủi ro an ninh mạng, các tài liệu minh chứng.
	II.1.4. Xử lý rủi ro an ninh mạng	II.1.4.1. Thực hiện các biện pháp xử lý rủi ro an ninh mạng và xây dựng phương án ứng phó khi rủi ro còn lại (sau khi đã xử lý) xảy ra	Chưa đáp ứng Mức 1.	Đã thực hiện tất cả các nội dung sau: - Thực hiện các biện pháp xử lý rủi ro an ninh mạng; - Xây dựng phương án ứng phó khi rủi ro còn lại (sau khi đã xử lý) xảy ra.	Đáp ứng Mức 1 và có cơ chế đo lường, đánh giá tính hiệu quả của các hoạt động sau: - Thực hiện các biện pháp xử lý rủi ro an ninh mạng; - Xây dựng phương án ứng phó khi rủi ro còn lại (sau khi đã xử lý) xảy ra.	Đáp ứng Mức 2 và có cơ chế cải tiến liên tục để tối ưu hoá các hoạt động sau: - Thực hiện các biện pháp xử lý rủi ro an ninh mạng; - Xây dựng phương án ứng phó khi rủi ro còn lại (sau khi đã xử lý) xảy ra.	Báo cáo kết quả thực hiện, các tài liệu minh chứng.
		II.1.4.2. Tần suất đánh giá và cải thiện hiệu quả của các biện pháp	Chưa đáp ứng Mức 3.			- Cấp độ 3: tối thiểu 01 lần/01 năm; - Cấp độ 4 trở lên: tối thiểu 01 lần/06 tháng.	Báo cáo kết quả thực hiện, các tài liệu minh chứng.

		kiểm soát được sử dụng để giảm thiểu rủi ro					
	II.1.5. Giám sát rủi ro an ninh mạng	II.1.5.1. Giám sát và cập nhật những thay đổi liên quan đến rủi ro đã được xác định, tối thiểu bao gồm: khả năng xảy ra, mức độ ảnh hưởng, mức độ rủi ro, tài sản bị ảnh hưởng, biện pháp kiểm soát đã áp dụng.	Chưa đáp ứng Mức 1.	Đã thực hiện giám sát và cập nhật những thay đổi liên quan đến rủi ro đã được xác định, tối thiểu bao gồm: khả năng xảy ra, mức độ ảnh hưởng, mức độ rủi ro, tài sản bị ảnh hưởng, biện pháp kiểm soát đã áp dụng.	Đáp ứng Mức 1 và có cơ chế đo lường, đánh giá tính hiệu quả của hoạt động giám sát và cập nhật những thay đổi liên quan đến rủi ro đã được xác định.	Đáp ứng Mức 2 và có cơ chế cải tiến liên tục để tối ưu hoá hoạt động giám sát và cập nhật những thay đổi liên quan đến rủi ro đã được xác định.	Báo cáo kết quả thực hiện, các tài liệu minh chứng.
	II.1.6. Truyền thông rủi ro an ninh mạng	II.1.6.1. Chia sẻ kết quả đánh giá rủi ro cho các bên liên quan (áp dụng đối với hệ thống thông tin cấp độ 4 trở lên)	Chưa đáp ứng Mức 1.	Có kế hoạch chia sẻ và đã chia sẻ kết quả đánh giá rủi ro cho các bên liên quan.	Đáp ứng Mức 1 và có cơ chế đo lường, đánh giá tính hiệu quả của hoạt động chia sẻ kết quả đánh giá rủi ro cho các bên liên quan.	Đáp ứng Mức 2 và có cơ chế cải tiến liên tục để tối ưu hoá hoạt động chia sẻ kết quả đánh giá rủi ro cho các bên liên quan.	Kế hoạch chia sẻ kết quả đánh giá rủi ro cho các bên liên quan, các tài liệu minh chứng.
		II.1.6.2. Thông báo kịp thời cho các bên liên quan về thay đổi quan trọng liên quan đến rủi ro	Chưa đáp ứng Mức 1.	Trong vòng 07 ngày kể từ khi phát hiện thay đổi.	Trong vòng 03 ngày kể từ khi phát hiện thay đổi.	Trong vòng 24 giờ kể từ khi phát hiện thay đổi.	Kế hoạch thông báo rủi ro cho các bên liên quan, các tài liệu minh chứng.
II.2. Quản lý tài sản phần cứng	II.2.1. Thiết lập và duy trì hệ thống quản lý danh mục tài sản phần cứng	II.2.1.1. Lập danh sách, theo dõi, cập nhật trạng thái của tất cả tài sản phần cứng có khả năng lưu trữ hoặc xử lý dữ liệu	Chưa đáp ứng Mức 1.	Đã lập danh sách, theo dõi, cập nhật trạng thái của tất cả tài sản phần cứng có khả năng lưu trữ hoặc xử lý dữ liệu, bao gồm: + Thiết bị của người dùng cuối (không áp dụng đối với thiết bị của người dùng cuối chỉ sử dụng	Có cơ chế kiểm soát đo lường, đánh giá tính hiệu quả của hoạt động lập danh sách, theo dõi, cập nhật trạng thái của tất cả tài sản phần cứng có khả năng lưu trữ hoặc xử lý dữ liệu.	Có cơ chế cải tiến liên tục để tối ưu hóa hoạt động lập danh sách, theo dõi, cập nhật trạng thái của tất cả tài sản phần cứng có khả năng lưu trữ hoặc xử lý dữ liệu.	Danh sách tài sản phần cứng, các tài liệu minh chứng

				dịch vụ và không có các quyền quản trị, quản lý) + Thiết bị di động, thiết bị lưu trữ ngoài + Thiết bị văn phòng, thiết bị mạng + Thiết bị OT/IoT + Máy chủ trong môi trường vật lý, ảo hóa, truy cập từ xa và điện toán đám mây.			
		II.2.1.2. Kiểm tra an ninh tất cả tài sản vật lý đưa vào sử dụng (áp dụng đối với hệ thống thông tin cấp độ 4 trở lên)	Chưa đáp ứng Mức 1.	Căn cứ vào điều kiện thực tế, tổ chức thực hiện kiểm tra an ninh tất cả tài sản vật lý đưa vào sử dụng.	Đáp ứng Mức 1 và có cơ chế đo lường, đánh giá tính hiệu quả của hoạt động kiểm tra an ninh tất cả tài sản vật lý .	Đáp ứng Mức 2 và có cơ chế cải tiến liên tục để tối ưu hoá hoạt động kiểm tra an ninh tất cả tài sản vật lý.	Danh sách tài sản vật lý được kiểm tra bởi cơ quan, tổ chức có thẩm quyền, biên bản, các tài liệu minh chứng.
		II.2.1.3. Tính đầy đủ của Danh sách tài sản phần cứng.	Chưa đáp ứng Mức 1.	Đáp ứng đầy đủ các yêu cầu sau: - Có danh sách tài sản phần cứng; - Danh sách đã bao gồm tối thiểu các thông tin cơ bản sau: tên tài sản, địa chỉ mạng IP (đối với thiết bị đặt địa chỉ IP tĩnh); địa chỉ phần cứng MAC/ mã nhận diện serial; thời gian ngừng hỗ trợ kỹ thuật của hãng (nếu có); vị trí lắp đặt địa lý, vị trí lắp đặt trong hệ thống mạng;	Đáp ứng Mức 1 và có cơ chế đo lường, đánh giá tính hiệu quả của hoạt động lập danh sách tài sản phần cứng.	Đáp ứng Mức 2 và có cơ chế cải tiến liên tục để tối ưu hóa hoạt động lập danh sách tài sản phần cứng.	Danh sách tài sản phần cứng, các tài liệu minh chứng.

				mục đích sử dụng, tình trạng sử dụng; - Tài sản vật lý đã được giao, gán trách nhiệm cho cá nhân hoặc bộ phận quản lý, sử dụng.			
		II.2.1.4. Quản lý các thiết bị di động kết nối vào hệ thống thông tin	Chưa đáp ứng Mức 1.	Đáp ứng đầy đủ các yêu cầu sau: - Có quy định thiết bị di động kết nối vào hệ thống thông tin được đăng ký để kiểm soát (không áp dụng đối với thiết bị của người dùng cuối chỉ sử dụng dịch vụ và không có các quyền quản trị, quản lý); - Có quy định trách nhiệm của cá nhân trong tổ chức khi sử dụng thiết bị di động để phục vụ công việc.	Đáp ứng Mức 1 và có cơ chế đo lường, đánh giá tính hiệu quả của hoạt động kiểm soát các thiết bị di động kết nối vào hệ thống thông tin	Đáp ứng Mức 2 và có cơ chế cải tiến liên tục để tối ưu hóa hoạt động kiểm soát các thiết bị di động kết nối vào hệ thống thông tin	Quy định, Danh sách các thiết bị di động kết nối vào hệ thống thông tin, các tài liệu minh chứng.
	II.2.2. Xử lý các tài sản phần cứng chưa được quản lý	II.2.2.1. Xây dựng, ban hành và đảm bảo tuân thủ quy trình phát hiện và xử lý các tài sản phần cứng không có trong danh sách quản lý	Chưa đáp ứng Mức 1.	Đã ban hành và đảm bảo tuân thủ quy trình phát hiện và xử lý các tài sản phần cứng không có trong danh sách quản lý, đang kết nối trái phép vào hệ thống thông tin định kỳ, trong đó: - Cấp độ 3: tối thiểu 01 lần/06 tháng; - Cấp độ 4: tối thiểu 01 lần/01 quý; - Cấp độ 5: tối thiểu 01 lần/01 tháng.	Đáp ứng Mức 1 và có cơ chế đo lường, đánh giá tính hiệu quả của quy trình phát hiện và xử lý các tài sản phần cứng không có trong danh sách quản lý.	Đáp ứng Mức 2 và có cơ chế cải tiến liên tục để tối ưu hoá quy trình phát hiện và xử lý các tài sản phần cứng không có trong danh sách quản lý.	Quy trình phát hiện tài sản trái phép, Kết quả thực hiện quy trình định kỳ (báo cáo/mail), các tài liệu minh chứng.

		II.2.2.2. Có thể lựa chọn loại bỏ, từ chối kết nối hoặc cách ly tài sản trái phép	Chưa đáp ứng Mức 1.	Có các phương án loại bỏ, từ chối kết nối hoặc cách ly tài sản trái phép.	Đáp ứng Mức 1 và có cơ chế đo lường, đánh giá tính hiệu quả của hoạt động loại bỏ, từ chối kết nối hoặc cách ly tài sản trái phép.	Đáp ứng Mức 2 và có cơ chế cải tiến liên tục để tối ưu hoá hoạt động loại bỏ, từ chối kết nối hoặc cách ly tài sản trái phép.	Phương án loại bỏ, từ chối kết nối hoặc cách ly tài sản trái phép, các tài liệu minh chứng.
	II.2.3. Rà soát các tài sản kết nối vào hệ thống thông tin (áp dụng đối với hệ thống thông tin cấp độ 4 trở lên)	II.2.3.1. Xây dựng, ban hành và đảm bảo tuân thủ quy định rà quét để phát hiện tài sản kết nối vào hệ thống thông tin	Chưa đáp ứng Mức 1.	Đã xây dựng, ban hành và đảm bảo tuân thủ quy định rà quét để phát hiện tài sản kết nối vào hệ thống thông tin định kỳ, trong đó: - Cấp độ 4: tối thiểu 01 lần/01 quý; - Cấp độ 5: tối thiểu 01 lần/01 tháng.	Đáp ứng Mức 1 và có cơ chế đo lường, đánh giá tính hiệu quả của quy định rà quét để phát hiện tài sản kết nối vào hệ thống thông tin.	Đáp ứng Mức 2 và có cơ chế cải tiến liên tục để tối ưu hoá quy định rà quét để phát hiện tài sản kết nối vào hệ thống thông tin.	Quy định rà quét để phát hiện tài sản kết nối vào hệ thống thông tin, các tài liệu minh chứng.
		II.2.3.2. Thực hiện cập nhật danh sách tài sản dựa trên kết quả rà quét	Chưa đáp ứng Mức 1.	Đã thực hiện cập nhật danh sách tài sản dựa trên kết quả rà quét.	Đáp ứng Mức 1 và có cơ chế đo lường, đánh giá tính hiệu quả của hoạt động cập nhật danh sách tài sản dựa trên kết quả rà quét.	Đáp ứng Mức 2 và có cơ chế cải tiến liên tục để tối ưu hoá hoạt động cập nhật danh sách tài sản dựa trên kết quả rà quét.	Báo cáo kết quả cập nhật danh sách tài sản, các tài liệu minh chứng.
	II.2.4. Xử lý các tài sản phần cứng khi chuyển giao	II.2.4.1. Có phương án xóa sạch thông tin, dữ liệu trên tài sản phần cứng khi chuyển giao hoặc thay đổi mục đích sử dụng.	Chưa đáp ứng Mức 1.	Đã có phương án xóa sạch thông tin, dữ liệu trên tài sản phần cứng khi chuyển giao hoặc thay đổi mục đích sử dụng.	Đáp ứng Mức 1 và có cơ chế đo lường, đánh giá tính hiệu quả của hoạt động xóa sạch thông tin, dữ liệu trên tài sản phần cứng khi chuyển giao hoặc thay đổi mục đích sử dụng.	Đáp ứng Mức 2 và có cơ chế cải tiến liên tục để tối ưu hoá hoạt động xóa sạch thông tin, dữ liệu trên tài sản phần cứng khi chuyển giao hoặc thay đổi mục đích sử dụng.	

	II.2.5. Giải pháp cập nhật, kiểm kê tài sản công nghệ thông tin	II.2.5.1. Sử dụng tính năng ghi nhật ký DHCP trên tất cả các máy chủ DHCP hoặc công cụ quản lý địa chỉ mạng IP (nếu có)	Chưa đáp ứng Mức 1.	Đã sử dụng tính năng ghi nhật ký DHCP trên tất cả các máy chủ DHCP hoặc công cụ quản lý địa chỉ mạng IP (nếu có).	Đáp ứng Mức 1 và có cơ chế đo lường, đánh giá tính hiệu quả của hoạt động sử dụng tính năng ghi nhật ký DHCP trên tất cả các máy chủ DHCP hoặc công cụ quản lý địa chỉ mạng IP (nếu có).	Đáp ứng Mức 2 và có cơ chế cải tiến liên tục để tối ưu hoá hoạt động sử dụng tính năng ghi nhật ký DHCP trên tất cả các máy chủ DHCP hoặc công cụ quản lý địa chỉ mạng IP (nếu có).	Nhật ký DHCP, nhật ký của công cụ quản lý địa chỉ mạng IP được cấu hình, các tài liệu minh chứng.
		II.2.5.2. Tiến hành rà soát nhật ký để cập nhật danh sách tài sản công nghệ thông tin định kỳ	Chưa đáp ứng Mức 1.	Đã thực hiện rà soát nhật ký để cập nhật danh sách tài sản công nghệ thông tin định kỳ, trong đó: - Cấp độ 3: tối thiểu 01 lần/06 tháng; - Cấp độ 4: tối thiểu 01 lần/01 quý; - Cấp độ 5: tối thiểu 01 lần/01 tháng.	Đáp ứng Mức 1 và có cơ chế đo lường, đánh giá tính hiệu quả của hoạt động rà soát nhật ký để cập nhật danh sách tài sản công nghệ thông tin.	Đáp ứng Mức 2 và có cơ chế cải tiến liên tục để tối ưu hoá hoạt động rà soát nhật ký để cập nhật danh sách tài sản công nghệ thông tin.	Danh sách cập nhật tài sản công nghệ thông tin được rà soát.
	II.2.6. Quản lý tài sản thanh lý/ hư hỏng (áp dụng đối với hệ thống thông tin cấp độ 4 trở lên)	II.2.6.1. Xây dựng, ban hành và đảm bảo tuân thủ quy trình thanh lý/ tiêu hủy tài sản CNTT	Chưa đáp ứng Mức 1.	Đã ban hành quy trình thanh lý/ tiêu hủy tài sản CNTT	Đáp ứng Mức 1 và có cơ chế đo lường, đánh giá tính hiệu quả của quy trình thanh lý/ tiêu hủy tài sản CNTT.	Đáp ứng Mức 2 và có cơ chế cải tiến liên tục để tối ưu hoá quy trình thanh lý/ tiêu hủy tài sản CNTT.	Quy trình thanh lý/tiêu hủy tài sản CNTT, các tài liệu minh chứng.
		II.2.6.2. Có biện pháp chuyên dụng để xóa sạch thông tin, dữ liệu trên máy chủ khi chuyển giao hoặc thay đổi mục đích sử dụng	Chưa đáp ứng Mức 1.	Có biện pháp chuyên dụng để xóa sạch thông tin, dữ liệu trên máy chủ khi chuyển giao hoặc thay đổi mục đích sử dụng.	Đáp ứng Mức 1 và có cơ chế đo lường, đánh giá tính hiệu quả của biện pháp chuyên dụng để xóa sạch thông tin, dữ liệu.	Đáp ứng Mức 2 và có cơ chế cải tiến liên tục để tối ưu hoá biện pháp chuyên dụng để xóa sạch thông tin, dữ liệu.	Biện pháp chuyên dụng để xóa sạch thông tin, dữ liệu, tài liệu minh chứng.

		II.2.6.3. Sao lưu dự phòng thông tin, dữ liệu trên máy chủ, bản dự phòng hệ điều hành máy chủ trước khi thực hiện xóa dữ liệu, hệ điều hành (áp dụng đối với hệ thống thông tin cấp độ 5)	Chưa đáp ứng Mức 1.	Sao lưu dự phòng thông tin, dữ liệu trên máy chủ, bản dự phòng hệ điều hành máy chủ trước khi thực hiện xóa dữ liệu, hệ điều hành.	Đáp ứng Mức 1 và có cơ chế đo lường, đánh giá tính hiệu quả của hoạt động sao lưu dự phòng thông tin, dữ liệu.	Đáp ứng Mức 2 và có cơ chế cải tiến liên tục để tối ưu hoá hoạt động sao lưu dự phòng thông tin, dữ liệu.	Biên bản thực hiện, tài liệu minh chứng.
		II.2.6.4. Có biện pháp kiểm tra, bảo đảm dữ liệu không thể khôi phục sau khi xóa (áp dụng đối với hệ thống thông tin cấp độ 5)	Chưa đáp ứng Mức 1.	Có biện pháp kiểm tra, bảo đảm dữ liệu không thể khôi phục sau khi xóa.	Đáp ứng Mức 1 và có cơ chế đo lường, đánh giá tính hiệu quả của biện pháp kiểm tra.	Đáp ứng Mức 2 và có cơ chế cải tiến liên tục để tối ưu hoá biện pháp kiểm tra.	Biện pháp kiểm tra, báo cáo, tài liệu minh chứng.
II.3. Quản lý tài sản phần mềm	II.3.1. Thiết lập và duy trì hệ thống quản lý danh mục tài sản phần mềm	II.3.1.1. Lập danh sách, theo dõi, cập nhật trạng thái của tất cả tài sản phần mềm	Chưa đáp ứng Mức 1.	Đã lập danh sách, theo dõi, cập nhật trạng thái của tất cả tài sản phần mềm hiện đang được cài đặt trên các tài sản phần cứng thuộc hệ thống thông tin của cơ quan, tổ chức.	Đáp ứng Mức 1 và có cơ chế đo lường, đánh giá tính hiệu quả của hoạt động lập danh sách, theo dõi, cập nhật trạng thái của tất cả tài sản phần mềm hiện đang được cài đặt trên các tài sản phần cứng thuộc hệ thống thông tin của cơ quan, tổ chức.	Đáp ứng Mức 2 và có cơ chế cải tiến liên tục để tối ưu hóa hoạt động lập danh sách, theo dõi, cập nhật trạng thái của tất cả tài sản phần mềm hiện đang được cài đặt trên các tài sản phần cứng thuộc hệ thống thông tin của cơ quan, tổ chức.	Danh sách tài sản phần mềm, các tài liệu minh chứng.

		II.3.1.2. Tính đầy đủ của Danh sách tài sản phần mềm	Chưa đáp ứng Mức 1.	Đáp ứng tất cả các yêu cầu sau: - Đã lập danh sách tài sản phần mềm; - Danh sách tài sản phần mềm bao gồm tối thiểu các thông tin cơ bản sau: tên tài sản, mục đích sử dụng, thời gian ngừng hỗ trợ kỹ thuật (nếu có), phạm vi sử dụng, chủ thể quản lý, thông tin về bản quyền, phiên bản, hệ thống thông tin thành phần (nếu có). Tài sản phần mềm được gắn trách nhiệm cho cá nhân hoặc bộ phận quản lý, sử dụng.	Đáp ứng Mức 1 và có cơ chế đo lường, đánh giá tính hiệu quả của hoạt động lập danh sách tài sản phần mềm.	Đáp ứng Mức 2 và có cơ chế cải tiến liên tục để tối ưu hóa hoạt động lập danh sách tài sản phần mềm.	Danh sách tài sản phần mềm đầy đủ các thông tin cơ bản, các tài liệu minh chứng.
	II.3.2. Thiết lập và duy trì danh sách các tài sản phần mềm được phép sử dụng	II.3.2.1. Lập danh sách, theo dõi, cập nhật danh sách các phần mềm được phép sử dụng trong hệ thống thông tin của cơ quan, tổ chức	Chưa đáp ứng Mức 1.	Đã lập danh sách, theo dõi, cập nhật danh sách các phần mềm được phép sử dụng trong hệ thống thông tin của cơ quan, tổ chức	Đáp ứng Mức 1 và có cơ chế đo lường, đánh giá tính hiệu quả của hoạt động lập danh sách, theo dõi, cập nhật danh sách các phần mềm được phép sử dụng trong hệ thống thông tin của cơ quan, tổ chức	Đáp ứng Mức 2 và có cơ chế cải tiến liên tục để tối ưu hóa hoạt động lập danh sách, theo dõi, cập nhật danh sách các phần mềm được phép sử dụng trong hệ thống thông tin của cơ quan, tổ chức	Danh sách phần mềm được phép sử dụng, các tài liệu minh chứng.
		II.3.2.2. Tính đầy đủ của Danh sách các phần mềm được phép sử dụng	Chưa đáp ứng Mức 1.	Đáp ứng tất cả các yêu cầu sau: - Đã lập danh sách các phần mềm được phép sử dụng; - Danh sách phần mềm được phép sử dụng bao gồm các phần mềm được	Đáp ứng Mức 1 và có cơ chế đo lường, đánh giá tính hiệu quả của hoạt động lập danh sách phần mềm được phép sử dụng.	Đáp ứng Mức 2 và có cơ chế cải tiến liên tục để tối ưu hóa hoạt động lập danh sách phần mềm được phép sử dụng.	Danh sách các phần mềm được phép sử dụng, các tài liệu minh chứng.

				cung cấp bởi nhà cung cấp dịch vụ, các môi trường thực thi cần cài đặt cho ứng dụng.			
		II.3.2.3. Xây dựng, ban hành và đảm bảo tuân thủ quy định kiểm soát việc cài đặt và sử dụng các phần mềm đã được cấp phép	Chưa đáp ứng Mức 1.	Đáp ứng tất cả các yêu cầu sau: - Đã xây dựng, ban hành và đảm bảo tuân thủ quy định kiểm soát việc cài đặt và sử dụng các phần mềm đã được cấp phép; - Quy định kiểm soát việc cài đặt và sử dụng các phần mềm được cấp phép chưa đáp ứng: Đảm bảo giới hạn đặc quyền tối thiểu các quyền quản trị trên các tài sản CNTT; Ngăn chặn các tác vụ thực thi, vô hiệu hóa, cài đặt và gỡ bỏ phần mềm, thư viện, đoạn mã lệnh trái phép trên hệ thống; Có phương án kỹ thuật để theo dõi hoạt động cài đặt chương trình phần mềm trên các tài sản CNTT; - Có cơ chế đảm bảo tuân thủ quy định.	Đáp ứng Mức 1 và có cơ chế đo lường, đánh giá tính hiệu quả của việc thực hiện quy định kiểm soát việc cài đặt và sử dụng các phần mềm đã được cấp phép.	Đáp ứng Mức 2 và có cơ chế cải tiến liên tục để tối ưu hoá quy định kiểm soát việc cài đặt và sử dụng các phần mềm đã được cấp phép.	Quy định kiểm soát cài đặt và sử dụng các phần mềm đã được cấp phép, các tài liệu minh chứng.
		II.3.2.4. Định kỳ đánh giá và cập nhật danh sách phần mềm được phép sử dụng	Chưa đáp ứng Mức 3.			Đã thực hiện định kỳ đánh giá và cập nhật danh sách phần mềm được phép sử dụng hoặc khi xảy ra các thay đổi trong tổ	Bản cập nhật danh sách phần mềm được phép sử dụng.

						chức ảnh hưởng đến danh sách, trong đó: - Cấp độ 3, 4: tối thiểu 01 lần/01 năm; - Cấp độ 5: tối thiểu 01 lần/06 tháng.	
	II.3.3. Đảm bảo toàn bộ các tài sản phần mềm được phép sử dụng đang trong thời gian hỗ trợ của nhà cung cấp (áp dụng đối với hệ thống thông tin cấp độ 4 trở lên)	II.3.3.1. Thực hiện định kỳ rà soát danh sách tài sản phần mềm được phép sử dụng và danh sách tài sản phần mềm cài đặt trên các tài sản phần cứng	Chưa đáp ứng Mức 1.	Thực hiện định kỳ rà soát danh sách tài sản phần mềm được phép sử dụng và danh sách tài sản phần mềm cài đặt trên các tài sản phần cứng để đảm bảo tất cả tài sản phần mềm đang trong thời gian hỗ trợ của nhà cung cấp, trong đó: - Cấp độ 4: tối thiểu 01 lần/01 năm; - Cấp độ 5: tối thiểu 01 lần/06 tháng.	Đáp ứng Mức 1 và có cơ chế đo lường, đánh giá tính hiệu quả của hoạt động rà soát danh sách tài sản phần mềm được phép sử dụng và danh sách tài sản phần mềm cài đặt trên các tài sản phần cứng.	Đáp ứng Mức 2 và có cơ chế cải tiến liên tục để tối ưu hoá hoạt động rà soát danh sách tài sản phần mềm được phép sử dụng và danh sách tài sản phần mềm cài đặt trên các tài sản phần cứng.	Kết quả rà soát định kỳ danh sách tài sản phần mềm, các tài liệu minh chứng.
	II.3.4. Xử lý các tài sản phần mềm trái phép	II.3.4.1. Xây dựng, ban hành và đảm bảo tuân thủ quy trình phát hiện và xử lý các phần mềm trái phép	Chưa đáp ứng Mức 1.	Đã xây dựng, ban hành và đảm bảo tuân thủ quy trình phát hiện và xử lý các phần mềm trái phép định kỳ, trong đó: - Cấp độ 3: tối thiểu 01 lần/01 năm; - Cấp độ 4: tối thiểu 01 lần/06 tháng; - Cấp độ 5: tối thiểu 01 lần/01 tháng.	Đáp ứng Mức 1 và có cơ chế đo lường, đánh giá tính hiệu quả của quy trình phát hiện và xử lý các phần mềm trái phép.	Đáp ứng Mức 2 và có cơ chế cải tiến liên tục để tối ưu hoá quy trình phát hiện và xử lý các phần mềm trái phép.	Quy trình phát hiện và xử lý các phần mềm trái phép, các tài liệu minh chứng.
		II.3.4.2. Những phần mềm trái phép nhưng vẫn cần thiết đối với hoạt động của	Chưa đáp ứng Mức 1.	Đáp ứng tất cả các yêu cầu sau: - Đã có danh sách ngoại lệ để quản lý những phần mềm trái phép nhưng vẫn cần thiết đối với hoạt	Đáp ứng Mức 1 và có cơ chế đo lường, đánh giá tính hiệu quả của việc lập danh sách ngoại lệ để quản lý những phần mềm	Đáp ứng Mức 2 và có cơ chế cải tiến liên tục để tối ưu hoá hoạt động lập danh sách ngoại lệ để quản lý những phần mềm trái	Danh sách ngoại lệ các phần mềm trái phép nhưng vẫn

		cơ quan, tổ chức được đưa vào danh sách ngoại lệ để quản lý		động của cơ quan, tổ chức; - Danh sách ngoại lệ cần thể hiện chi tiết các biện pháp kiểm soát giảm thiểu nguy cơ an ninh mạng ảnh hưởng đến hệ thống.	trái phép nhưng vẫn cần thiết đối với hoạt động của cơ quan, tổ chức.	phép nhưng vẫn cần thiết đối với hoạt động của cơ quan, tổ chức.	cần thiết, các tài liệu minh chứng.
		II.3.4.3. Xóa/ gỡ bỏ hoàn toàn những phần mềm trái phép không nằm trong danh sách ngoại lệ	Chưa đáp ứng Mức 1.	Có kế hoạch để xóa/ gỡ bỏ hoàn toàn những phần mềm trái phép không nằm trong danh sách ngoại lệ khỏi các tài sản phần cứng của cơ quan, tổ chức trong thời gian sớm nhất.	Đáp ứng Mức 1 và có cơ chế đo lường, đánh giá tính hiệu quả của hoạt động xóa/ gỡ bỏ hoàn toàn những phần mềm trái phép không nằm trong danh sách ngoại lệ.	Đáp ứng Mức 2 và có cơ chế cải tiến liên tục để tối ưu hoá hoạt động xóa/ gỡ bỏ hoàn toàn những phần mềm trái phép không nằm trong danh sách ngoại lệ.	Kế hoạch xóa/gỡ bỏ các phần mềm trái phép khỏi các tài sản phần cứng, các tài liệu minh chứng.
II.4. Quản lý tài sản thông tin	II.4.1. Thiết lập và duy trì quy định quản lý tài sản thông tin	II.4.1.1. Xây dựng, ban hành và đảm bảo tuân thủ quy định quản lý tài sản thông tin	Chưa đáp ứng Mức 1.	Đáp ứng tất cả các yêu cầu sau: - Đã ban hành quy định quản lý tài sản thông tin, trong đó, xác định danh sách tài sản thông tin, mức độ nhạy cảm, chủ sở hữu, các bước xử lý, thời gian lưu trữ và các yêu cầu khi tiêu hủy/xóa bỏ dựa trên các tiêu chuẩn về mức độ bảo mật của tài sản thông tin; - Có cơ chế đảm bảo tuân thủ quy định;	Đáp ứng Mức 1 và có cơ chế kiểm soát đo lường, đánh giá tính hiệu quả của việc thực hiện quy định quản lý tài sản thông tin.	Đáp ứng Mức 2 và có cơ chế cải tiến liên tục để tối ưu hoá quy định quản lý tài sản thông tin.	Quy định quản lý tài sản thông tin, các tài liệu minh chứng.
		II.4.1.2. Quy định về các	Chưa đáp ứng Mức 1.	Đã có quy định về các mức độ nhạy cảm của tài	Đáp ứng Mức 1 và có cơ chế đo lường, đánh giá tính hiệu hiệu	Đáp ứng Mức 2 và có cơ chế cải tiến liên tục để tối ưu hoá quy	Quy định về các mức độ nhạy cảm của tài sản thông

		mức độ nhạy cảm của tài sản thông tin		sản thông tin, có thể quy định như sau: - Mức 1: Công khai. Tài sản thông tin công khai không yêu cầu về bảo mật; - Mức 2: Nội bộ. Tài sản thông tin nội bộ yêu cầu chỉ những người trong tổ chức mới có quyền truy cập; - Mức 3: Hạn chế truy cập. Tài sản thông tin bị hạn chế yêu cầu quyền truy cập, chỉ những người dùng được cấp quyền mới có thể truy cập vào dữ liệu. Việc tiết lộ tài sản thông tin bị hạn chế truy cập có khả năng ảnh hưởng đến hoạt động của các đơn vị; - Mức 4: Bí mật nhà nước. Thông tin có nội dung quan trọng, do cơ quan, tổ chức có thẩm quyền xác định; chưa công khai, nếu bị lộ, bị mất có thể gây nguy hại đến lợi ích quốc gia, dân tộc (thực hiện theo quy định của Luật Bảo vệ bí mật nhà nước).	quả của việc thực hiện quy định về các mức độ nhạy cảm của hệ thống thông tin.	định về các mức độ nhạy cảm của hệ thống thông tin.	tin, các tài liệu minh chứng.
		II.4.1.3. Xây dựng quy trình yêu cầu truy cập, thêm mới,	Chưa đáp ứng Mức 1.	Đã ban hành quy trình yêu cầu truy cập, thêm mới, sửa, xóa dữ liệu để	Đáp ứng Mức 1 và có cơ chế đo lường, đánh giá tính hiệu quả của quy trình yêu	Đáp ứng Mức 2 và có cơ chế cải tiến liên tục để tối ưu hoá quy trình yêu cầu truy	Quy trình yêu cầu truy cập, thêm mới, sửa. Xóa dữ liệu

		sửa, xóa dữ liệu để kiểm soát truy cập dữ liệu		kiểm soát truy cập dữ liệu.	cầu truy cập, thêm mới, sửa, xóa dữ liệu để kiểm soát truy cập dữ liệu.	cập, thêm mới, sửa, xóa dữ liệu để kiểm soát truy cập dữ liệu.	
		II.4.1.4. Kiểm tra cấp độ phân quyền dữ liệu định kỳ	Chưa đáp ứng Mức 1.	Đã kiểm tra cấp độ phân quyền dữ liệu định kỳ, trong đó: - Cấp độ 3: tối thiểu 01 lần/06 tháng; - Cấp độ 4: tối thiểu 01 lần/01 quý; - Cấp độ 5: tối thiểu 01 lần/01 tháng.	Đáp ứng Mức 1 và có cơ chế đo lường, đánh giá tính hiệu quả của hoạt động kiểm tra cấp độ phân quyền dữ liệu.	Đáp ứng Mức 2 và có cơ chế cải tiến liên tục để tối ưu hoá hoạt động kiểm tra cấp độ phân quyền dữ liệu.	Biên bản, tài liệu minh chứng.
		II.4.1.5. Đánh giá và cập nhật quy trình quản lý tài sản thông tin	Chưa đáp ứng Mức 1.	Đã thực hiện đánh giá và cập nhật quy trình quản lý tài sản thông tin định kỳ hoặc khi xảy ra các thay đổi trong tổ chức ảnh hưởng đến quy trình, trong đó: - Cấp độ 3, 4: tối thiểu 01 lần/01 năm; - Cấp độ 5: tối thiểu 01 lần/06 tháng.	Đáp ứng Mức 1 và có cơ chế đo lường, đánh giá tính hiệu quả của quy trình quản lý tài sản thông tin.	Đáp ứng Mức 2 và có cơ chế cải tiến liên tục để tối ưu hoá quy trình quản lý tài sản thông tin.	Báo cáo, tài liệu minh chứng.
	II.4.2. Thiết lập và duy trì danh sách tài sản thông tin	II.4.2.1. Lập danh sách các tài sản thông tin dựa trên quy trình quản lý tài sản thông tin	Chưa đáp ứng Mức 1.	Đã có danh sách các tài sản thông tin dựa trên quy trình quản lý tài sản thông tin.	Đáp ứng Mức 1 và có cơ chế kiểm soát đo lường, đánh giá tính hiệu quả của hoạt động lập danh sách các tài sản thông tin dựa trên quy trình quản lý tài sản thông tin.	Đáp ứng Mức 2 và có cơ chế cải tiến liên tục để tối ưu hoá hoạt động lập danh sách các tài sản thông tin dựa trên quy trình quản lý tài sản thông tin.	Danh sách tài sản thông tin
		II.4.2.2. Đánh giá và cập nhật danh sách tài sản thông tin	Chưa đáp ứng Mức 1.	Đã thực hiện đánh giá và cập nhật danh sách tài sản thông tin hoặc khi xảy ra thay đổi trong tổ chức ảnh hưởng đến danh sách, trong đó:	Đáp ứng Mức 1 và có cơ chế kiểm soát đo lường, đánh giá tính hiệu quả của hoạt động đánh giá và cập	Đáp ứng Mức 2 và có cơ chế cải tiến liên tục để tối ưu hoá hoạt động đánh giá và cập nhật danh sách tài sản thông tin.	Bản đánh giá, tài liệu minh chứng.

				- Cấp độ 3, 4: tối thiểu 01 lần/01 năm; - Cấp độ 5: tối thiểu 01 lần/06 tháng.	nhật danh sách tài sản thông tin.		
	II.4.3. Xây dựng danh sách kiểm soát truy cập tài sản thông tin	II.4.3.1. Xây dựng danh sách quyền truy cập của các tài khoản, người dùng đối với từng loại tài sản thông tin	Chưa đáp ứng Mức 1.	Có danh sách quyền truy cập của các tài khoản, người dùng đối với từng loại tài sản thông tin.	Đáp ứng Mức 1 và có cơ chế đo lường, đánh giá tính hiệu quả của hoạt động xây dựng danh sách quyền truy cập của các tài khoản, người dùng đối với từng loại tài sản thông tin.	Đáp ứng Mức 2 và có cơ chế cải tiến liên tục để tối ưu hoá hoạt động xây dựng danh sách quyền truy cập của các tài khoản, người dùng đối với từng loại tài sản thông tin.	Danh sách quyền truy cập các tài khoản, người dùng đối với từng loại tài sản thông tin
	II.4.4. Mã hóa dữ liệu quan trọng	II.4.4.1. Mã hóa dữ liệu quan trọng được lưu trữ trong các tài sản phần cứng và phần mềm của cơ quan, tổ chức	Chưa đáp ứng Mức 1.	Đã thực hiện mã hóa dữ liệu quan trọng được lưu trữ trong các tài sản phần cứng và phần mềm của cơ quan, tổ chức.	Đáp ứng Mức 1 và có cơ chế đo lường, đánh giá tính hiệu quả của các hoạt động mã hóa dữ liệu quan trọng được lưu trữ trong các tài sản phần cứng và phần mềm của cơ quan, tổ chức.	Đáp ứng Mức 2 và có cơ chế cải tiến liên tục để tối ưu hoá hoạt động mã hóa dữ liệu quan trọng được lưu trữ trong các tài sản phần cứng và phần mềm của cơ quan, tổ chức.	Dữ liệu lưu trữ được mã hóa
		II.4.4.2. Mã hoá dữ liệu quan trọng trong quá trình truyền gửi	Chưa đáp ứng Mức 1.	Đã thực hiện mã hoá dữ liệu quan trọng trong quá trình truyền gửi.	Đáp ứng Mức 1 và có cơ chế đo lường, đánh giá tính hiệu quả của hoạt động mã hoá dữ liệu quan trọng trong quá trình truyền gửi.	Đáp ứng Mức 2 và có cơ chế cải tiến liên tục để tối ưu hoá hoạt động mã hoá dữ liệu quan trọng trong quá trình truyền gửi.	Dữ liệu trong quá trình truyền gửi được mã hóa
		II.4.4.3. Thực hiện bảo vệ và quản lý vòng đời mã khóa sử dụng để mã hóa dữ liệu	Chưa đáp ứng Mức 1.	Đã thực hiện bảo vệ và quản lý vòng đời mã khóa sử dụng để mã hóa dữ liệu.	Đáp ứng Mức 1 và có cơ chế đo lường, đánh giá tính hiệu quả của hoạt động bảo vệ và quản lý vòng đời mã khóa sử	Đáp ứng Mức 2 và có cơ chế cải tiến liên tục để tối ưu hoá hoạt động bảo vệ và quản lý vòng đời mã khóa	Báo cáo, tài liệu chứng minh.

					dụng để mã hóa dữ liệu.	sử dụng để mã hóa dữ liệu.	
		II.4.4.4. Mã hóa dữ liệu tối thiểu 02 lần khi truyền qua môi trường mạng (áp dụng đối với hệ thống thông tin cấp độ 4 trở lên)	Chưa đáp ứng Mức 1.	Sử dụng kết hợp các kết nối mạng an toàn, các biện pháp mã hóa hoặc biện pháp kiểm soát rủi ro tương đương để bảo đảm dữ liệu quan trọng được mã hóa tối thiểu 02 lần khi truyền qua môi trường mạng.	Đáp ứng Mức 1 và có cơ chế đo lường, đánh giá tính hiệu quả của hoạt động mã hóa dữ liệu tối thiểu 02 lần.	Đáp ứng Mức 2 và có cơ chế cải tiến liên tục để tối ưu hoá hoạt động mã hóa dữ liệu tối thiểu 02 lần.	Thuyết minh, tài liệu minh chứng.
		II.4.4.5. Sử dụng các phương pháp mã hóa mạnh (áp dụng đối với hệ thống thông tin cấp độ 4 trở lên)	Chưa đáp ứng Mức 1.	Sử dụng các phương pháp mã hóa mạnh (chưa được các tổ chức quốc tế công bố điểm yếu) để mã hóa dữ liệu.	Đáp ứng Mức 1 và có cơ chế đo lường, đánh giá tính hiệu quả của hoạt động sử dụng các phương pháp mã hóa mạnh.	Đáp ứng Mức 2 và có cơ chế cải tiến liên tục để tối ưu hoá hoạt động sử dụng các phương pháp mã hóa mạnh.	Thuyết minh, tài liệu minh chứng.
		II.4.4.6. Sử dụng thiết bị phần cứng chuyên dụng (áp dụng đối với hệ thống thông tin cấp độ 5)	Chưa đáp ứng Mức 1.	Sử dụng thiết bị phần cứng chuyên dụng để phục vụ mã hóa và giải mã.	Đáp ứng Mức 1 và có cơ chế đo lường, đánh giá tính hiệu quả của việc sử dụng thiết bị phần cứng chuyên dụng.	Đáp ứng Mức 2 và có cơ chế cải tiến liên tục để tối ưu hoá việc sử dụng thiết bị phần cứng chuyên dụng.	Thuyết minh, tài liệu minh chứng.
	II.4.5. Nguyên vẹn dữ liệu (áp dụng đối với hệ thống thông tin cấp độ 4 trở lên)	II.4.5.1. Phương án quản lý, lưu trữ dữ liệu quan trọng trong hệ thống cùng với mã	Chưa đáp ứng Mức 1.	Có phương án quản lý, lưu trữ dữ liệu quan trọng trong hệ thống cùng với mã kiểm tra tính nguyên vẹn.	Đáp ứng Mức 1 và có cơ chế đo lường, đánh giá tính hiệu quả của phương án quản lý, lưu trữ dữ liệu quan trọng trong hệ thống cùng	Đáp ứng Mức 2 và có cơ chế cải tiến liên tục để tối ưu hoá phương án quản lý, lưu trữ dữ liệu quan trọng trong hệ thống	Thuyết minh, tài liệu minh chứng.

		kiểm tra tính nguyên vẹn			với mã kiểm tra tính nguyên vẹn.	cùng với mã kiểm tra tính nguyên vẹn.	
		II.4.5.2. Phương án giám sát, cảnh báo khi có thay đổi thông tin, dữ liệu	Chưa đáp ứng Mức 1.	Có phương án giám sát, cảnh báo khi có thay đổi thông tin, dữ liệu lưu trên hệ thống lưu trữ/phương tiện lưu trữ.	Đáp ứng Mức 1 và có cơ chế đo lường, đánh giá tính hiệu quả của phương án giám sát, cảnh báo khi có thay đổi thông tin, dữ liệu.	Đáp ứng Mức 2 và có cơ chế cải tiến liên tục để tối ưu hoá phương án giám sát, cảnh báo khi có thay đổi thông tin, dữ liệu.	Thuyết minh, tài liệu minh chứng.
		II.4.5.3. Phương án khôi phục tính nguyên vẹn của dữ liệu	Chưa đáp ứng Mức 1.	Có phương án khôi phục tính nguyên vẹn của dữ liệu.	Đáp ứng Mức 1 và có cơ chế đo lường, đánh giá tính hiệu quả của phương án khôi phục tính nguyên vẹn của dữ liệu.	Đáp ứng Mức 2 và có cơ chế cải tiến liên tục để tối ưu hoá phương án khôi phục tính nguyên vẹn của dữ liệu.	Thuyết minh, tài liệu minh chứng.
	II.4.6. Tài liệu hóa luồng dữ liệu	II.4.6.1. Có tài liệu mô tả các luồng dữ liệu quan trọng	Chưa đáp ứng Mức 1.	Có tài liệu mô tả các luồng dữ liệu quan trọng.	Đáp ứng Mức 1 và có cơ chế đo lường, đánh giá tính hiệu quả của hoạt động xây dựng tài liệu mô tả các luồng dữ liệu quan trọng.	Đáp ứng Mức 2 và có cơ chế cải tiến liên tục để tối ưu hoá hoạt động xây dựng tài liệu mô tả các luồng dữ liệu quan trọng.	Tài liệu mô tả luồng dữ liệu quan trọng
		II.4.6.2. Xây dựng và tuân thủ quy định quản lý phiên bản tài liệu tại tổ chức	Chưa đáp ứng Mức 1.	Đáp ứng tất cả các yêu cầu sau: - Ban hành quy định quản lý phiên bản tài liệu tại tổ chức; - Có cơ chế đảm bảo tuân thủ quy định.	Đáp ứng Mức 1 và có cơ chế đo lường, đánh giá tính hiệu quả của việc thực hiện quy định quản lý phiên bản tài liệu tại tổ chức.	Đáp ứng Mức 2 và có cơ chế cải tiến liên tục để tối ưu hoá quy định quản lý phiên bản tài liệu tại tổ chức.	Quy định quản lý phiên bản tài liệu tại tổ chức
		II.4.6.3. Đánh giá và cập nhật quy định, tài liệu.	Chưa đáp ứng Mức 1.	Đã thực hiện đánh giá và cập nhật quy định, tài liệu định kỳ tối thiểu 01 lần/01 năm hoặc khi có thay đổi trong tổ chức ảnh hưởng đến tài liệu.	Đáp ứng Mức 1 và có cơ chế đo lường, đánh giá tính hiệu quả của hoạt động đánh giá và cập nhật quy định, tài liệu.	Đáp ứng Mức 2 và có cơ chế cải tiến liên tục để tối ưu hoá hoạt động đánh giá và cập nhật quy định, tài liệu.	Bản cập nhật tài liệu mô tả luồng dữ liệu

	II.4.7. Tách biệt quá trình xử lý và lưu trữ dữ liệu quan trọng	II.4.7.1. Có quy định về việc xử lý dữ liệu quan trọng.	Chưa đáp ứng Mức 1.	Đáp ứng tất cả các yêu cầu sau: - Đã ban hành quy định về việc xử lý dữ liệu quan trọng; - Có cơ chế đảm bảo tuân thủ quy định.	Đáp ứng Mức 1 và có cơ chế đo lường, đánh giá tính hiệu quả của việc thực hiện quy định về việc xử lý dữ liệu quan trọng.	Đáp ứng Mức 2 và có cơ chế cải tiến liên tục để tối ưu hoá quy định về việc xử lý dữ liệu quan trọng.	Quy định xử lý dữ liệu quan trọng.
		II.4.7.2. Tách biệt tài sản/môi trường xử lý, lưu trữ dữ liệu có độ nhạy cảm cao, dữ liệu quan trọng với dữ liệu có độ nhạy cảm thấp	Chưa đáp ứng Mức 1.	Đáp ứng tất cả các yêu cầu sau: - Tách biệt tài sản/môi trường xử lý, lưu trữ dữ liệu có độ nhạy cảm cao, dữ liệu quan trọng với dữ liệu có độ nhạy cảm thấp (về mặt logic hoặc vật lý) hoặc có phương án kiểm soát rủi ro tương đương đảm bảo an ninh dữ liệu. - Không sử dụng các tài sản/ môi trường dành cho dữ liệu nhạy cảm thấp để lưu trữ và xử lý dữ liệu có mức độ nhạy cảm cao.	Đáp ứng Mức 1 và có cơ chế đo lường, đánh giá tính hiệu quả của các hoạt động tách biệt tài sản/môi trường xử lý, lưu trữ dữ liệu có độ nhạy cảm cao, dữ liệu quan trọng với dữ liệu có độ nhạy cảm thấp.	Đáp ứng Mức 2 và có cơ chế cải tiến liên tục để tối ưu hoá hoạt động tách biệt tài sản/môi trường xử lý, lưu trữ dữ liệu có độ nhạy cảm cao, dữ liệu quan trọng với dữ liệu có độ nhạy cảm thấp.	Thuyết minh, tài liệu minh chứng.
		II.4.7.3. Sử dụng kênh vật lý riêng để bảo mật dữ liệu (áp dụng đối với hệ thống thông tin cấp độ 4 trở lên)	Chưa đáp ứng Mức 1.	Sử dụng kênh vật lý riêng hoặc có phương án kiểm soát rủi ro tương đương để bảo mật dữ liệu quan trọng, dữ liệu có độ nhạy cảm cao khi truyền đưa, trao đổi qua môi trường mạng.	Đáp ứng Mức 1 và có cơ chế đo lường, đánh giá tính hiệu quả của các hoạt động sử dụng kênh vật lý riêng để bảo mật dữ liệu.	Đáp ứng Mức 2 và có cơ chế cải tiến liên tục để tối ưu hoá hoạt động sử dụng kênh vật lý riêng để bảo mật dữ liệu.	Thuyết minh, tài liệu minh chứng.
	II.4.8. Triển khai giải pháp phòng chống thất thoát dữ liệu (áp dụng đối với hệ thống thông tin	II.4.8.1. Xây dựng và triển khai giải pháp phòng chống thất thoát dữ liệu	Chưa đáp ứng Mức 1.	Đã xây dựng và triển khai giải pháp phòng chống thất thoát dữ liệu đối với dữ liệu có độ nhạy cảm mức 03 trở lên, dữ liệu quan trọng được lưu trữ,	Đáp ứng Mức 1 và có cơ chế đo lường, đánh giá tính hiệu quả của hoạt động xây dựng và triển khai giải pháp phòng	Đáp ứng Mức 2 và có cơ chế cải tiến liên tục để tối ưu hoá giải pháp chống thất thoát dữ liệu.	Giải pháp chống thất thoát dữ liệu

	cấp độ 4 trở lên)			xử lý trong hệ thống thông tin.	chống thất thoát dữ liệu.		
	II.4.9. Lưu trữ nhật ký truy cập dữ liệu quan trọng (áp dụng đối với hệ thống thông tin cấp độ 4 trở lên)	II.4.9.1. Ghi lại nhật ký hành vi đối dữ liệu có độ nhạy cảm cao, dữ liệu quan trọng	Chưa đáp ứng Mức 1.	Đã thực hiện ghi lại nhật ký hành vi đối với dữ liệu có độ nhạy cảm cao, dữ liệu quan trọng được lưu trữ, xử lý trong hệ thống thông tin.	Đáp ứng Mức 1 và có cơ chế đo lường, đánh giá tính hiệu quả của hoạt động ghi lại nhật ký hành vi đối với dữ liệu có độ nhạy cảm cao, dữ liệu quan trọng	Đáp ứng Mức 2 và có cơ chế cải tiến liên tục để tối ưu hoá hoạt động ghi lại nhật ký hành vi đối dữ liệu có độ nhạy cảm cao, dữ liệu quan trọng	Thuyết minh, tài liệu minh chứng.
		II.4.9.2. Rà soát nhật ký thường xuyên	Chưa đáp ứng Mức 1.	Đã thực hiện rà soát nhật ký thường xuyên để phát hiện sớm những hành vi truy cập trái phép, trong đó: - Cấp độ 4: tối thiểu 01 lần/01 quý; - Cấp độ 5: tối thiểu 01 lần/01 tháng.	Đáp ứng Mức 1 và có cơ chế đo lường, đánh giá tính hiệu quả của hoạt động rà soát nhật ký thường xuyên.	Đáp ứng Mức 2 và có cơ chế cải tiến liên tục để tối ưu hoá hoạt động rà soát nhật ký thường xuyên.	Kết quả rà soát nhật ký 01 lần/tháng
	II.4.10. Sử dụng chữ ký số khi trao đổi thông tin số, dữ liệu số quan trọng	II.4.10.1. Sử dụng chữ ký số khi trao đổi dữ liệu có độ nhạy cảm cao, dữ liệu quan trọng	Chưa đáp ứng Mức 1.	Đáp ứng tất cả các yêu cầu sau: - Đã sử dụng chữ ký số khi trao đổi dữ liệu có độ nhạy cảm cao, dữ liệu quan trọng; - Đối với hệ thống thông tin cấp độ 4 trở lên: chữ ký số được cung cấp bởi cơ quan có thẩm quyền hoặc đơn vị cung cấp dịch vụ chữ ký số được cấp phép; có phương án bảo đảm an ninh mạng trong việc quản lý và sử dụng chữ ký số. - Đối với hệ thống thông tin cấp độ 5, sử dụng thiết	Đáp ứng Mức 1 và có cơ chế đo lường, đánh giá tính hiệu quả của hoạt động sử dụng chữ ký số khi trao đổi thông tin số, dữ liệu số quan trọng.	Đáp ứng Mức 2 và có cơ chế cải tiến liên tục để tối ưu hoá hoạt động sử dụng chữ ký số khi trao đổi thông tin số, dữ liệu số quan trọng.	Tài liệu/bằng chứng chứng minh.

				bị, phương tiện chuyên dụng để thực hiện ký và giải mã thông tin, dữ liệu khi gửi và nhận.			
II.5. Cấu hình an toàn cho phần cứng và phần mềm	II.5.1. Thiết lập và duy trì quy định, quy trình cấu hình an toàn cho tài sản phần cứng và phần mềm	II.5.1.1. Xây dựng, ban hành và đảm bảo tuân thủ quy định, quy trình cấu hình an toàn cho các tài sản phần cứng và phần mềm của cơ quan, tổ chức	Chưa đáp ứng Mức 1.	Đáp ứng tất cả các yêu cầu sau: - Đã ban hành quy định, quy trình cấu hình an toàn cho các tài sản phần cứng và phần mềm của cơ quan, tổ chức; - Có cơ chế đảm bảo tuân thủ quy định, quy trình.	Đáp ứng Mức 1 và có cơ chế đo lường, đánh giá tính hiệu quả của việc thực hiện quy định, quy trình cấu hình an toàn cho các tài sản phần cứng và phần mềm của cơ quan, tổ chức.	Đáp ứng Mức 2 và có cơ chế cải tiến liên tục để tối ưu hoá quy định, quy trình cấu hình an toàn cho các tài sản phần cứng và phần mềm của cơ quan, tổ chức.	Quy định, quy trình cấu hình an toàn
		II.5.1.2. Có các tài liệu cấu hình tiêu chuẩn, tài liệu cấu hình bảo mật nâng cao cho các tài sản phần cứng và phần mềm của cơ quan, tổ chức	Chưa đáp ứng Mức 1.	Đáp ứng tất cả các yêu cầu sau: - Có các tài liệu cấu hình tiêu chuẩn, tài liệu cấu hình bảo mật nâng cao cho các tài sản phần cứng và phần mềm của cơ quan, tổ chức; - Đảm bảo sử dụng giao thức kết nối an toàn, thiết lập tường lửa cho máy chủ/ máy trạm và có phương án chống đăng nhập tự động đối với các tài sản xử lý và lưu trữ dữ liệu quan trọng.	Đáp ứng Mức 1 và có cơ chế đo lường, đánh giá tính hiệu quả của việc thực hiện theo các tài liệu cấu hình tiêu chuẩn, tài liệu cấu hình bảo mật nâng cao cho các tài sản phần cứng và phần mềm của cơ quan, tổ chức.	Đáp ứng Mức 2 và có cơ chế cải tiến liên tục để tối ưu hoá các tài liệu cấu hình tiêu chuẩn, tài liệu cấu hình bảo mật nâng cao cho các tài sản phần cứng và phần mềm của cơ quan, tổ chức.	Tài liệu cấu hình, tài liệu chứng minh
		II.5.1.3. Vô hiệu hóa các giao thức mạng không an toàn, các dịch vụ mà phần cứng,	Chưa đáp ứng Mức 1.	Đã vô hiệu hóa các giao thức mạng không an toàn, các dịch vụ mà phần cứng, phần mềm không sử dụng.	Đáp ứng Mức 1 và có cơ chế đo lường, đánh giá tính hiệu quả của hoạt động vô hiệu hóa các giao thức mạng không an	Đáp ứng Mức 2 và có cơ chế cải tiến liên tục để tối ưu hoá hoạt động vô hiệu hóa các giao thức mạng không an toàn, các	Báo cáo thực hiện, tài liệu minh chứng.

		phần mềm không sử dụng			toàn, các dịch vụ mà phần cứng, phần mềm không sử dụng.	dịch vụ mà phần cứng, phần mềm không sử dụng.	
		II.5.1.4. Cấu hình tối ưu và tăng cường bảo mật cho tài sản phần cứng trước khi đưa vào vận hành, khai thác	Chưa đáp ứng Mức 1.	Đã cấu hình tối ưu và tăng cường bảo mật cho tài sản phần cứng trước khi đưa vào vận hành, khai thác.	Đáp ứng Mức 1 và có cơ chế đo lường, đánh giá tính hiệu quả của hoạt động cấu hình tối ưu và tăng cường bảo mật cho tài sản phần cứng trước khi đưa vào vận hành, khai thác.	Đáp ứng Mức 2 và có cơ chế cải tiến liên tục để tối ưu hoá hoạt động cấu hình tối ưu và tăng cường bảo mật cho tài sản phần cứng trước khi đưa vào vận hành, khai thác.	Báo cáo thực hiện, tài liệu minh chứng.
		II.5.1.5. Đánh giá và cập nhật quy định, quy trình quản lý cấu hình an toàn và các tài liệu liên quan	Chưa đáp ứng Mức 1.	Đã thực hiện đánh giá và cập nhật quy định, quy trình quản lý cấu hình an toàn và các tài liệu liên quan tối thiểu 01 lần/năm hoặc khi có thay đổi xảy ra trong tổ chức ảnh hưởng đến tài liệu.	Đáp ứng Mức 1 và có cơ chế đo lường, đánh giá tính hiệu quả của hoạt động đánh giá và cập nhật quy định, quy trình quản lý cấu hình an toàn và các tài liệu liên quan.	Đáp ứng Mức 2 và có cơ chế cải tiến liên tục để tối ưu hoá hoạt động đánh giá và cập nhật quy định, quy trình quản lý cấu hình an toàn và các tài liệu liên quan.	Cập nhật quy định, quy trình tối thiểu 01 lần/năm
	II.5.2. Cấu hình tự động khóa phiên làm việc trên các tài sản phần cứng và phần mềm	II.5.2.1. Cấu hình tự động khóa phiên làm việc trên các tài sản phần cứng và phần mềm	Chưa đáp ứng Mức 1.	Dựa trên yêu cầu sử dụng, kết quả đánh giá rủi ro, thực hiện cấu hình tự động khóa phiên làm việc trên các tài sản phần cứng và phần mềm. Có thể thực hiện cấu hình như sau: - Tự động khóa phiên làm việc trên các tài sản sau một khoảng thời gian không sử dụng: + Đối với máy tính người dùng: không quá 15 phút. + Đối với các phiên quản trị phần mềm, máy chủ,	Đáp ứng Mức 1 và có cơ chế đo lường, đánh giá tính hiệu quả của hoạt động cấu hình tự động khóa phiên làm việc trên các tài sản phần cứng và phần mềm.	Đáp ứng Mức 2 và có cơ chế cải tiến liên tục để tối ưu hoá hoạt động cấu hình tự động khóa phiên làm việc trên các tài sản phần cứng và phần mềm.	Báo cáo thực hiện, tài liệu minh chứng.

				thiết bị mạng, thiết bị IoT: không quá 05 phút. + Đối với thiết bị di động: không quá 05 phút. + Đối với các phần mềm nghiệp vụ xử lý dữ liệu quan trọng: không quá 15 phút. - Tự động khóa thiết bị di động sau một số lần đăng nhập thất bại: + Đối với máy tính xách tay: tối đa 10 lần. + Đối với điện thoại: tối đa 10 lần. + Đối với các phần mềm nghiệp vụ lưu trữ và xử lý dữ liệu quan trọng: tối đa 05 lần. + Giới hạn thời gian mở khóa thiết bị sau khi bị khóa: tối thiểu 12 giờ, tối đa 30 ngày.			
		II.5.2.2. Có cơ chế mở khóa khẩn cấp dành cho quản trị viên/tài khoản đặc quyền	Chưa đáp ứng Mức 1.	Có cơ chế mở khóa khẩn cấp dành cho quản trị viên/tài khoản đặc quyền.	Đáp ứng Mức 1 và có cơ chế đo lường, đánh giá tính hiệu quả của cơ chế mở khóa khẩn cấp dành cho quản trị viên/tài khoản đặc quyền.	Đáp ứng Mức 2 và có cơ chế cải tiến liên tục để tối ưu hoá cơ chế mở khóa khẩn cấp dành cho quản trị viên/tài khoản đặc quyền.	Cơ chế mở khóa khẩn cấp, tài liệu minh chứng.
	II.5.3. Gỡ bỏ hoặc vô hiệu hoá các tính năng, dịch vụ	II.5.3.1. Xây dựng, ban hành và đảm bảo tuân thủ quy	Chưa đáp ứng Mức 1.	Đáp ứng tất cả các yêu cầu sau: - Đã ban hành quy định gỡ bỏ hoặc vô hiệu hoá các tính năng, dịch vụ	Đáp ứng Mức 1 và có cơ chế đo lường, đánh giá tính hiệu quả của việc thực hiện quy định gỡ bỏ	Đáp ứng Mức 2 và có cơ chế cải tiến liên tục để tối ưu hoá quy định gỡ bỏ hoặc vô hiệu hoá các tính	Quy định gỡ bỏ các tính năng, dịch vụ không cần thiết trên các tài sản

	không cần thiết trên các tài sản phần cứng và phần mềm (áp dụng đối với hệ thống thông tin cấp độ 4 trở lên)	định gỡ bỏ hoặc vô hiệu hoá các tính năng, dịch vụ không cần thiết trên các tài sản phần cứng và phần mềm.		không cần thiết trên các tài sản phần cứng và phần mềm; - Có cơ chế đảm bảo tuân thủ quy định.	hoặc vô hiệu hoá các tính năng, dịch vụ không cần thiết trên các tài sản phần cứng và phần mềm.	năng, dịch vụ không cần thiết trên các tài sản phần cứng và phần mềm.	phần cứng và phần mềm.
	II.5.4. Cấu hình máy chủ DNS tin cậy (áp dụng đối với hệ thống thông tin cấp độ 4 trở lên)	II.5.4.1. Thiết lập các cấu hình máy chủ DNS tin cậy trên các tài sản phần cứng nếu có.	Chưa đáp ứng Mức 1.	Đã thiết lập các cấu hình máy chủ DNS tin cậy trên các tài sản phần cứng nếu có.	Đáp ứng Mức 1 và có cơ chế đo lường, đánh giá tính hiệu quả của hoạt động thiết lập các cấu hình máy chủ DNS tin cậy trên các tài sản phần cứng nếu có.	Đáp ứng Mức 2 và có cơ chế cải tiến liên tục để tối ưu hoá hoạt động thiết lập các cấu hình máy chủ DNS tin cậy trên các tài sản phần cứng nếu có.	Cam kết bảo mật đối với các bên thuê khoán. Cung cấp mã nguồn phần mềm
	II.5.5. Thiết lập khả năng xóa sạch dữ liệu từ xa trên thiết bị di động cấp cho người dùng (áp dụng đối với hệ thống thông tin cấp độ 4 trở lên)	II.5.5.1. Xây dựng và triển khai giải pháp xóa sạch dữ liệu từ xa trên thiết bị di động cấp cho người dùng	Chưa đáp ứng Mức 1.	Đã xây dựng và triển khai giải pháp xóa sạch dữ liệu từ xa trên thiết bị di động của cơ quan, tổ chức, doanh nghiệp cấp cho người dùng.	Đáp ứng Mức 1 và có cơ chế đo lường, đánh giá tính hiệu quả của hoạt động xây dựng và triển khai giải pháp xóa sạch dữ liệu từ xa trên thiết bị di động cấp cho người dùng.	Đáp ứng Mức 2 và có cơ chế cải tiến liên tục để tối ưu hoá giải pháp xóa sạch dữ liệu từ xa trên thiết bị di động cấp cho người dùng.	Giải pháp xóa sạch dữ liệu từ xa trên thiết bị di động
	II.5.6. Phân tách các không gian làm việc riêng biệt trên các thiết bị di động cấp cho người dùng (áp dụng đối với hệ	II.5.6.1. Xây dựng, ban hành và đảm bảo tuân thủ quy định tách biệt các không gian làm việc riêng biệt trên thiết	Chưa đáp ứng Mức 1.	Đáp ứng tất cả các yêu cầu sau: - Đã thiết lập và ban hành quy định tách biệt các không gian làm việc riêng biệt trên thiết bị di động cấp cho người dùng;	Đáp ứng Mức 1 và có cơ chế đo lường, đánh giá tính hiệu quả của việc thực hiện quy định tách biệt các không gian làm việc riêng biệt	Đáp ứng Mức 2 và có cơ chế cải tiến liên tục để tối ưu hoá quy định tách biệt các không gian làm việc riêng biệt trên thiết bị	Quy định tách biệt không gian làm việc riêng biệt trên thiết bị di động

	thống thông tin cấp độ 4 trở lên)	bị di động cấp cho người dùng		- Có cơ chế đảm bảo tuân thủ quy định.	trên thiết bị di động cấp cho người dùng.	di động cấp cho người dùng.	
		II.5.6.2. Xây dựng giải pháp kỹ thuật cho phép quản lý thiết bị di động khi người dùng sử dụng hoặc kết nối tới các hệ thống của tổ chức (áp dụng đối với hệ thống thông tin cấp độ 5)	Chưa đáp ứng Mức 1.	Đã xây dựng giải pháp kỹ thuật cho phép quản lý thiết bị di động khi người dùng sử dụng hoặc kết nối tới các hệ thống của tổ chức.	Đáp ứng Mức 1 và có cơ chế đo lường, đánh giá tính hiệu quả của giải pháp kỹ thuật cho phép quản lý thiết bị di động khi người dùng sử dụng hoặc kết nối tới các hệ thống của tổ chức.	Đáp ứng Mức 2 và có cơ chế cải tiến liên tục để tối ưu hoá giải pháp kỹ thuật cho phép quản lý thiết bị di động khi người dùng sử dụng hoặc kết nối tới các hệ thống của tổ chức.	Giải pháp kỹ thuật quản lý thiết bị di động khi người dùng sử dụng hoặc kết nối
II.6. Quản lý tài khoản và quyền truy cập tài khoản của người dùng	II.6.1. Thiết lập và duy trì hệ thống quản lý tài khoản	II.6.1.1. Lập danh sách, theo dõi và cập nhật tất cả các tài khoản trên các tài sản phần cứng và phần mềm của tổ chức	Chưa đáp ứng Mức 1.	Đã lập danh sách, theo dõi và cập nhật tất cả các tài khoản trên các tài sản phần cứng và phần mềm của tổ chức.	Đáp ứng Mức 1 và có cơ chế đo lường, đánh giá tính hiệu quả của hoạt động lập danh sách, theo dõi và cập nhật tất cả các tài khoản trên các tài sản phần cứng và phần mềm của tổ chức.	Đáp ứng Mức 2 và có cơ chế cải tiến liên tục để tối ưu hoá hoạt động lập danh sách, theo dõi và cập nhật tất cả các tài khoản trên các tài sản phần cứng và phần mềm của tổ chức.	Danh sách tài khoản
		II.6.1.2. Tính toàn diện của danh sách tài khoản	Chưa đáp ứng Mức 1.	Danh sách tài khoản đã bao gồm tối thiểu các loại tài khoản sau: tài khoản quản trị, tài khoản tác nghiệp và tài khoản kỹ thuật.	Đáp ứng Mức 1 và có cơ chế đo lường, đánh giá tính hiệu quả của hoạt động đảm bảo danh sách tài khoản bao gồm tối thiểu các loại tài khoản sau: tài khoản quản trị, tài khoản tác	Đáp ứng Mức 2 và có cơ chế cải tiến liên tục để tối ưu hoá hoạt động đảm bảo danh sách tài khoản bao gồm tối thiểu các loại tài khoản sau: tài khoản quản trị, tài	Danh sách tài khoản tối thiểu 03 loại tài khoản: quản trị, tác nghiệp, kỹ thuật

					nghiệp và tài khoản kỹ thuật.	khoản tác nghiệp và tài khoản kỹ thuật.	
		II.6.1.3. Tính đầy đủ của các trường thông tin và tính hợp lệ của các tài khoản trong danh sách tài khoản.	Chưa đáp ứng Mức 1.	Đáp ứng tất cả các yêu cầu sau: - Danh sách tài khoản đã bao gồm các thông tin tối thiểu: loại tài khoản, tên tài khoản, trạng thái tài khoản, tên tài sản/ hệ thống thông tin tương ứng, tên người quản lý, phòng ban, ngày kích hoạt tài khoản, ngày vô hiệu hoá tài khoản (nếu có); - Có cơ chế đảm bảo tất cả tài khoản đang hoạt động là hợp lệ.	Đáp ứng Mức 1 và có cơ chế đo lường, đánh giá tính hiệu quả của hoạt động đảm bảo danh sách tài khoản bao gồm các thông tin tối thiểu, đảm bảo tất cả tài khoản đang hoạt động là hợp lệ.	Đáp ứng Mức 2 và có cơ chế cải tiến liên tục để tối ưu hoá hoạt động đảm bảo danh sách tài khoản bao gồm các thông tin tối thiểu, đảm bảo tất cả tài khoản đang hoạt động là hợp lệ.	Danh sách tài khoản bao gồm các thông tin tối thiểu như yêu cầu.
		II.6.1.4. Danh sách tài khoản được rà soát định kỳ	Chưa đáp ứng Mức 3.			Danh sách tài khoản được rà soát định kỳ, trong đó: - Cấp độ 3: tối thiểu 01 lần/06 tháng; - Cấp độ 4: tối thiểu 01 lần/01 quý; - Cấp độ 5: tối thiểu 01 lần/01 tháng	Báo cáo rà soát danh sách tài khoản, tài liệu minh chứng.
	II.6.2. Xây dựng và tuân thủ quy định sử dụng mật khẩu	II.6.2.1. Thiết lập cấu hình mật khẩu trên tài sản phần cứng, phần mềm để đảm bảo an toàn mật khẩu người sử dụng	Chưa đáp ứng Mức 1.	Đã thiết lập cấu hình mật khẩu trên tài sản phần cứng, phần mềm để đảm bảo an toàn mật khẩu người sử dụng, bao gồm các yêu cầu sau: - Yêu cầu thay đổi mật khẩu mặc định.	Đáp ứng Mức 1 và có cơ chế đo lường, đánh giá tính hiệu quả của hoạt động thiết lập cấu hình mật khẩu trên tài sản phần cứng, phần mềm để đảm bảo an toàn mật khẩu người sử dụng.	Đáp ứng Mức 2 và có cơ chế cải tiến liên tục để tối ưu hoá hoạt động thiết lập cấu hình mật khẩu trên tài sản phần cứng, phần mềm để đảm bảo an toàn mật khẩu người sử dụng.	Báo cáo thực hiện, tài liệu minh chứng.

				- Thiết lập quy tắc đặt mật khẩu về số ký tự, loại ký tự. - Thiết lập thời gian yêu cầu thay đổi mật khẩu. - Thiết lập thời gian mật khẩu hợp lệ.			
		II.6.2.2. Triển khai quy định sử dụng mật khẩu an toàn trong tổ chức	Chưa đáp ứng Mức 1.	Dựa trên yêu cầu sử dụng, kết quả đánh giá rủi ro, triển khai quy định sử dụng mật khẩu an toàn trong tổ chức. Có thể thực hiện cấu hình như sau: - Sử dụng mật khẩu duy nhất cho mỗi tài sản hoặc sử dụng giải pháp xác thực và quản lý tập trung. - Yêu cầu thay đổi mật khẩu trong lần đăng nhập đầu tiên. - Đối với các hệ thống sử dụng xác thực MFA, quy định mật khẩu có tối thiểu 08 ký tự. - Đối với các hệ thống không sử dụng xác thực MFA, quy định mật khẩu có tối thiểu 14 ký tự, bao gồm ký tự viết thường, ký tự viết hoa, ký tự đặc biệt, chữ số. - Đối với tài khoản quản trị cần triển khai xác thực MFA, thay đổi mật khẩu định kỳ tối thiểu 01 lần/02 tháng và mật khẩu	Đáp ứng Mức 1 và có cơ chế đo lường, đánh giá tính hiệu quả của hoạt động triển khai quy định sử dụng mật khẩu an toàn trong tổ chức.	Đáp ứng Mức 2 và có cơ chế cải tiến liên tục để tối ưu hoá hoạt động triển khai quy định sử dụng mật khẩu an toàn trong tổ chức.	Báo cáo kết quả triển khai quy định sử dụng mật khẩu dựa trên kết quả đánh giá rủi ro, tài liệu minh chứng.

				mới không được trùng với 10 mật khẩu trước đó.			
	II.6.3. Xây dựng và tuân thủ quy định quản lý tài khoản	II.6.3.1. Xây dựng, ban hành và đảm bảo tuân thủ quy định quản lý tài khoản trong tổ chức	Chưa đáp ứng Mức 1.	Có quy định quản lý tài khoản trong tổ chức đáp ứng các yêu cầu sau: - Quản lý tài khoản tập trung; - Thay đổi hoặc vô hiệu hóa tài khoản mặc định trên phần mềm, thiết bị (như tài khoản root, administrator, tài khoản cấu hình sẵn của nhà cung cấp dịch vụ); - Quản lý tách biệt giữa các loại tài khoản: tài khoản quản trị, tài khoản tác nghiệp, tài khoản kỹ thuật, tài khoản dịch vụ; - Mỗi tài khoản truy cập hệ thống được gán cho một người sử dụng duy nhất; trường hợp chia sẻ tài khoản dùng chung, việc chia sẻ được phê duyệt bởi cấp có thẩm quyền và làm rõ trách nhiệm cá nhân tại mỗi thời điểm sử dụng; - Xóa hoặc vô hiệu hoá các tài khoản không hoạt động sau 45 ngày hoặc ngay khi có thay đổi về nhân sự quản lý tài khoản. - Đối với hệ thống thông tin cấp độ 4 trở lên, có	Đáp ứng Mức 1 và có cơ chế đo lường, đánh giá tính hiệu quả của việc thực hiện quy định quản lý tài khoản trong tổ chức.	Đáp ứng Mức 2 và có cơ chế cải tiến liên tục để tối ưu hoá quy định quản lý tài khoản trong tổ chức.	Quy định quản lý tài khoản trong tổ chức, tài liệu minh chứng.

				quy định về quản lý thiết bị lưu khóa bí mật và khóa bí mật.			
		II.6.3.2. Rà soát và cập nhật quy định quản lý tài khoản và các tài liệu liên quan	Chưa đáp ứng Mức 3.			Đã rà soát và cập nhật quy định quản lý tài khoản và các tài liệu liên quan tối thiểu 01 lần/01 năm hoặc khi có thay đổi trong tổ chức có ảnh hưởng đến quy định.	Bản cập nhật quy định quản lý tài khoản và các tài liệu liên quan.
	II.6.4. Xây dựng và tuân thủ quy định về quản lý truy cập	II.6.4.1. Xây dựng, ban hành và đảm bảo tuân thủ quy định về quản lý truy cập	Chưa đáp ứng Mức 1.	Đáp ứng tất cả các yêu cầu sau: - Đã xây dựng, ban hành và đảm bảo tuân thủ quy định về quản lý truy cập đáp ứng các yêu cầu sau: + Nguyên tắc cấp quyền tối thiểu và phân tách nhiệm vụ đối với mọi loại tài khoản; + Tài liệu hóa các quyền truy cập cần thiết tương ứng với các chức danh, bộ phận trong cơ quan, tổ chức; + Yêu cầu xác thực đa nhân tố đối với truy cập của người dùng từ bên ngoài tổ chức, từ đối tác/ bên thứ ba, từ internet và truy cập vào tài khoản có quyền quản trị hệ thống; - Có cơ chế đảm bảo tuân thủ quy định.	Đáp ứng Mức 1 và có cơ chế đo lường, đánh giá tính hiệu quả của việc thực hiện quy định về quản lý truy cập.	Đáp ứng Mức 2 và có cơ chế cải tiến liên tục để tối ưu hoá quy định về quản lý truy cập.	Quy định quản lý truy cập, tài liệu minh chứng.

		II.6.4.2. Rà soát và cập nhật quy định quản lý truy cập và các tài liệu liên quan	Chưa đáp ứng Mức 3.			Đã rà soát và cập nhật quy định quản lý truy cập và các tài liệu liên quan tối thiểu 01 lần/01 năm hoặc khi có thay đổi trong tổ chức có ảnh hưởng đến quy định.	Báo cáo, tài liệu chứng minh.
	II.6.5. Xây dựng và tuân thủ quy trình cấp mới, thay đổi và thu hồi quyền truy cập (áp dụng đối với hệ thống thông tin cấp độ 4 trở lên)	II.6.5.1. Xây dựng, ban hành và đảm bảo tuân thủ quy trình cấp mới, thay đổi và thu hồi quyền truy cập vào các tài sản CNTT của cơ quan, tổ chức.	Chưa đáp ứng Mức 1.	Đáp ứng tất cả các yêu cầu sau: - Đã xây dựng, ban hành và đảm bảo tuân thủ quy trình cấp mới, thay đổi và thu hồi quyền truy cập vào các tài sản CNTT của cơ quan, tổ chức; - Có cơ chế đảm bảo tuân thủ quy trình.	Đáp ứng Mức 1 và có cơ chế đo lường, đánh giá tính hiệu quả của quy trình cấp mới, thay đổi và thu hồi quyền truy cập vào các tài sản CNTT của cơ quan, tổ chức.	Đáp ứng Mức 2 và có cơ chế cải tiến liên tục để tối ưu hoá quy trình cấp mới, thay đổi và thu hồi quyền truy cập vào các tài sản CNTT của cơ quan, tổ chức.	Quy trình cấp mới, thay đổi và thu hồi quyền truy cập
		II.6.5.2. Định kỳ rà soát quy trình và công tác thực hiện cấp quyền truy cập vào các tài sản CNTT của cơ quan, tổ chức	Chưa đáp ứng Mức 1.			Đã rà soát quy trình và công tác thực hiện cấp quyền truy cập vào các tài sản CNTT của cơ quan, tổ chức hoặc khi có thay đổi trong tổ chức có ảnh hưởng đến quy trình, trong đó: - Cấp độ 4: tối thiểu 01 lần/01 năm; - Cấp độ 5: tối thiểu 01 lần/06 tháng	Báo cáo rà soát.
II.7. Quản lý lỗ hổng bảo mật	II.7.1. Thiết lập, tuân thủ và duy trì quy	II.7.1.1. Xây dựng, ban hành và đảm bảo tuân thủ quy	Chưa đáp ứng Mức 1.	Đáp ứng tất cả các yêu cầu sau: - Đã xây dựng, ban hành và đảm bảo tuân thủ quy	Đáp ứng Mức 1 và có cơ chế đo lường, đánh giá tính hiệu quả của quy trình quản lý lỗ	Đáp ứng Mức 2 và có cơ chế cải tiến liên tục để tối ưu hoá quy trình quản lý lỗ hổng	Quy trình quản lý lỗ hổng bảo mật đảm bảo các yêu cầu

	trình quản lý lỗ hổng bảo mật	trình quản lý lỗ hổng bảo mật cho các tài sản công nghệ thông tin của tổ chức		trình quản lý lỗ hổng bảo mật cho các tài sản công nghệ thông tin của tổ chức, bao gồm tối thiểu các bước: + Phát hiện lỗ hổng bảo mật: Xây dựng và triển khai giải pháp để rà quét lỗ hổng bảo mật cho các tài sản phần cứng và phần mềm của cơ quan, tổ chức; + Đánh giá mức độ nghiêm trọng của lỗ hổng: Triển khai đánh giá mức độ nghiêm trọng của lỗ hổng, từ đó xác định mức độ ưu tiên của việc khắc phục lỗ hổng; + Chia sẻ thông tin lỗ hổng: Thiết lập và duy trì cơ chế để chia sẻ thông tin, tiếp nhận và phản hồi báo cáo lỗ hổng bảo mật từ bên liên quan hoặc các nguồn công khai khác; + Triển khai các biện pháp khắc phục: Xây dựng phương án, kế hoạch khắc phục cho các lỗ hổng đã phát hiện theo thứ tự ưu tiên và đánh giá lại hệ thống để đảm bảo lỗ hổng đã được khắc phục hoàn toàn; - Có cơ chế đảm bảo tuân thủ quy trình.	hổng bảo mật cho các tài sản công nghệ thông tin của tổ chức.	bảo mật cho các tài sản công nghệ thông tin của tổ chức.	

		II.7.1.2. Rà soát và cập nhật quy trình quản lý lỗ hổng bảo mật	Chưa đáp ứng Mức 3.			Đã thực hiện rà soát và cập nhật quy trình và rà quét lỗ hổng bảo mật định kỳ hoặc khi xảy ra thay đổi trong tổ chức ảnh hưởng đến quy trình này, trong đó: - Cấp độ 3, 4: tối thiểu 01 lần/06 tháng; - Cấp độ 5: tối thiểu 01 lần/01 quý	Báo cáo rà quét, tài liệu minh chứng.
	II.7.2. Thiết lập, tuân thủ và duy trì quy trình quản lý bản vá	II.7.2.1. Xây dựng, ban hành và đảm bảo tuân thủ quy trình quản lý bản vá	Chưa đáp ứng Mức 1.	Đáp ứng tất cả các yêu cầu sau: - Đã xây dựng, ban hành quy trình quản lý bản vá, đáp ứng tối thiểu các yêu cầu sau: + Xây dựng và triển khai máy chủ quản lý bản vá tập trung cho toàn bộ tài sản phần cứng và phần mềm thuộc hệ thống thông tin; + Đánh giá tác động, tiến hành kiểm thử và xây dựng phương án phục hồi trước khi triển khai bản vá trên các hệ thống thông tin có xử lý hoặc lưu trữ dữ liệu quan trọng; + Thực hiện kiểm tra và cập nhật bản vá hệ điều hành, ứng dụng cho toàn	Đáp ứng Mức 1 và có cơ chế đo lường, đánh giá tính hiệu quả của quy trình quản lý bản vá.	Đáp ứng Mức 2 và có cơ chế cải tiến liên tục để tối ưu hoá quy trình quản lý bản vá.	Quy trình quản lý bản vá.

				bộ máy tính, thiết bị di động cấp cho người dùng tối thiểu 01 lần/01 tháng (nếu có); + Giám sát và duy trì hệ thống để đảm bảo phát hiện kịp thời các lỗ hổng mới xuất hiện và cập nhật bản vá; - Có cơ chế đảm bảo tuân thủ quy trình.			
II.8. Quản lý nhật ký an ninh mạng	II.8.1. Thiết lập, tuân thủ và duy trì một quy trình quản lý nhật ký an ninh mạng	II.8.1.1. Xây dựng, ban hành và đảm bảo tuân thủ quy định quản lý nhật ký an ninh mạng	Chưa đáp ứng Mức 1.	Đáp ứng tất cả các yêu cầu sau: - Đã xây dựng, ban hành quy định quản lý nhật ký an ninh mạng, bao gồm: + Quy định về cách thức ghi nhật ký; + Quy định về việc thu thập, kiểm tra, lưu trữ nhật ký; + Quy định các loại nhật ký được thu thập. Thu thập tối thiểu các loại nhật ký sau: nhật ký truy cập hệ thống, nhật ký tiến trình hoạt động, nhật ký ứng dụng, nhật ký cảnh báo của các thiết bị bảo mật; + Nhật ký truy cập hệ thống tối thiểu bao gồm: địa chỉ nguồn (IP/ tên máy, tên miền), địa chỉ đích (IP/ tên máy, tên miền), tài khoản đích (tên	Đáp ứng Mức 1 và có cơ chế đo lường, đánh giá tính hiệu quả của việc thực hiện quy định quản lý nhật ký an ninh mạng.	Đáp ứng Mức 2 và có cơ chế cải tiến liên tục để tối ưu hoá quy định quản lý nhật ký an ninh mạng.	Quy trình quản lý nhật ký an ninh mạng

				người dùng/ mã định danh), thời điểm xảy ra, thông tin hành vi; + Nhật ký tiến trình hoạt động tối thiểu bao gồm: thông tin thiết bị (IP/ tên thiết bị, tên miền), thông tin tiến trình (tên, mã định danh, tiến trình cha, lệnh khởi tạo), tài khoản đích (tên người dùng/ mã định danh), thời điểm xảy ra; + Nhật ký cảnh báo tối thiểu bao gồm: tên cảnh báo, thiết bị, mức độ, địa chỉ nguồn, loại cảnh báo, thời điểm xảy ra; + Sử dụng máy chủ thời gian để đồng bộ thời gian giữa các thiết bị mạng, thiết bị đầu cuối và các thành phần khác trong hệ thống tham gia giám sát; + Sử dụng giải pháp SIEM hoặc có sản phẩm, phương án tương đương phục vụ quản lý và phân tích sự kiện an ninh mạng tập trung; + Lưu trữ và quản lý tập trung nhật ký hệ thống thu thập được từ các thiết bị hệ thống; + Đảm bảo duy trì không gian lưu trữ nhật ký tối			

				thiểu (cấp độ 3: 03 tháng, cấp độ 4: 06 tháng; cấp độ 5: 12 tháng). Triển khai hệ thống theo dõi tránh tình trạng đầy không gian lưu trữ, dẫn tới thất thoát dữ liệu; + Định kỳ thực hiện rà soát nhật ký an ninh mạng (cấp độ 3: tối thiểu 01 lần/ 06 tháng; cấp độ 4, 5: tối thiểu 01 lần/01 tháng); + Đối với hệ thống thông tin cấp độ 4 trở lên: *(1)*Nhật ký ứng dụng tối thiểu bao gồm: thông tin truy cập ứng dụng, thông tin đăng nhập khi quản trị ứng dụng, thông tin các lỗi phát sinh trong quá trình hoạt động, thông tin thay đổi cấu hình ứng dụng; *(2)*Nhật ký truy cập dữ liệu tối thiểu bao gồm: địa chỉ nguồn (IP/ tên máy, tên miền), địa chỉ đích (IP/ tên máy, tên miền), thông tin hành động (đọc, thêm, sửa, xóa, sao chép), tài khoản đích (tên người dùng/ mã định danh), thời điểm xảy ra; *(3)*Đảm bảo việc thu thập nhật ký được áp dụng trên toàn bộ tài sản CNTT; *(4)*Kết nối và gửi			

				nhật ký an ninh mạng từ đối tượng giám sát về hệ thống giám sát tập trung.			
		II.8.1.2. Kiểm tra và cập nhật quy định quản lý nhật ký an ninh mạng	Chưa đáp ứng Mức 3.			Đã kiểm tra và cập nhật quy định tối thiểu 01 lần/năm hoặc khi có thay đổi ảnh hưởng đến quy định này.	Bản cập nhật thay đổi.
	II.8.2. Thu thập nhật ký an ninh mạng của nhà cung cấp dịch vụ (áp dụng đối với hệ thống thông tin cấp độ 4 trở lên)	II.8.2.1. Thực hiện thu thập nhật ký an ninh mạng của các nhà cung cấp dịch vụ đối với các dịch vụ mà tổ chức sử dụng	Chưa đáp ứng Mức 1.	Đã có hoạt động thu thập nhật ký an ninh mạng của các nhà cung cấp dịch vụ đối với các dịch vụ mà tổ chức sử dụng.	Đáp ứng Mức 1 và có cơ chế đo lường, đánh giá tính hiệu quả của hoạt động thu thập nhật ký an ninh mạng của các nhà cung cấp dịch vụ đối với các dịch vụ mà tổ chức sử dụng.	Đáp ứng Mức 2 và có cơ chế cải tiến liên tục để tối ưu hoá hoạt động thu thập nhật ký an ninh mạng của các nhà cung cấp dịch vụ đối với các dịch vụ mà tổ chức sử dụng.	Tài liệu minh chứng.
	II.8.3. Bảo vệ nhật ký an ninh mạng (áp dụng đối với hệ thống thông tin cấp độ 4 trở lên)	II.8.3.1. Kiểm soát truy cập và ghi lại lịch sử tác động tới nhật ký an ninh mạng	Chưa đáp ứng Mức 1.	Đã có hoạt động kiểm soát truy cập và ghi lại lịch sử tác động tới nhật ký an ninh mạng.	Đáp ứng Mức 1 và có cơ chế đo lường, đánh giá tính hiệu quả của hoạt động kiểm soát truy cập và ghi lại lịch sử tác động tới nhật ký an ninh mạng.	Đáp ứng Mức 2 và có cơ chế cải tiến liên tục để tối ưu hoá hoạt động kiểm soát truy cập và ghi lại lịch sử tác động tới nhật ký an ninh mạng.	Biện pháp kiểm soát truy cập tới nhật ký an ninh mạng
		II.8.3.2. Đảm bảo nhật ký an ninh mạng không bị sửa đổi, xóa bỏ	Chưa đáp ứng Mức 1.	Đã có cơ chế đảm bảo nhật ký an ninh mạng không bị sửa đổi, xóa bỏ.	Đáp ứng Mức 1 và có cơ chế đo lường, đánh giá tính hiệu quả của hoạt động đảm bảo nhật ký an ninh mạng không bị sửa đổi, xóa bỏ.	Đáp ứng Mức 2 và có cơ chế cải tiến liên tục để tối ưu hoá hoạt động đảm bảo nhật ký an ninh mạng không bị sửa đổi, xóa bỏ.	Báo cáo, tài liệu chứng minh.

		II.8.3.3. Lưu trữ dữ liệu nhật ký hệ thống trên hệ thống riêng biệt không cùng phân vùng mạng với hệ thống phát sinh dữ liệu nhật ký	Chưa đáp ứng Mức 1.	Đã lưu trữ dữ liệu nhật ký hệ thống trên hệ thống riêng biệt không cùng phân vùng mạng với hệ thống phát sinh dữ liệu nhật ký, mã hóa với những dữ liệu nhật ký quan trọng (nếu có).	Đáp ứng Mức 1 và có cơ chế đo lường, đánh giá tính hiệu quả của hoạt động lưu trữ dữ liệu nhật ký hệ thống.	Đáp ứng Mức 2 và có cơ chế cải tiến liên tục để tối ưu hoá hoạt động lưu trữ dữ liệu nhật ký hệ thống.	Giải pháp lưu trữ dữ liệu nhật ký trên hệ thống riêng biệt
II.9. Bảo vệ cho trình duyệt web, dịch vụ thư điện tử	II.9.1. Quản lý trình duyệt web và dịch vụ thư điện tử	II.9.1.1. Có danh sách các trình duyệt web và dịch vụ thư điện tử được phép sử dụng trong cơ quan, tổ chức	Chưa đáp ứng Mức 1.	Đã ban hành và quản lý danh sách các trình duyệt web và dịch vụ thư điện tử được phép sử dụng trong cơ quan, tổ chức.	Đáp ứng Mức 1 và có cơ chế đo lường, đánh giá tính hiệu quả của hoạt động quản lý danh sách các trình duyệt web và dịch vụ thư điện tử được phép sử dụng trong cơ quan, tổ chức.	Đáp ứng Mức 2 và có cơ chế cải tiến liên tục để tối ưu hoá hoạt động quản lý danh sách các trình duyệt web và dịch vụ thư điện tử được phép sử dụng trong cơ quan, tổ chức.	Danh sách trình duyệt web và dịch vụ thư điện tử được phép sử dụng
		II.9.1.2. Đảm bảo danh sách các trình duyệt web và dịch vụ thư điện tử trên đang trong thời gian hỗ trợ của nhà cung cấp.	Chưa đáp ứng Mức 1.	Đã có cơ chế đảm bảo danh sách các trình duyệt web và dịch vụ thư điện tử đang trong thời gian hỗ trợ của nhà cung cấp.	Đáp ứng Mức 1 và có cơ chế đo lường, đánh giá tính hiệu quả của hoạt động đảm bảo danh sách các trình duyệt web và dịch vụ thư điện tử đang trong thời gian hỗ trợ của nhà cung cấp.	Đáp ứng Mức 2 và có cơ chế cải tiến liên tục để tối ưu hoá hoạt động đảm bảo danh sách các trình duyệt web và dịch vụ thư điện tử đang trong thời gian hỗ trợ của nhà cung cấp.	Danh sách trình duyệt web và dịch vụ thư điện tử đang trong thời gian hỗ trợ của nhà cung cấp.
		II.9.1.3. Sử dụng giải pháp đảm bảo an ninh mạng cho hệ thống thư điện tử hoặc có phương án tương đương	Chưa đáp ứng Mức 1.	Sử dụng giải pháp đảm bảo an ninh mạng cho hệ thống thư điện tử hoặc có phương án tương đương.	Đáp ứng Mức 1 và có cơ chế đo lường, đánh giá tính hiệu quả của giải pháp đảm bảo an ninh mạng cho hệ thống thư điện tử hoặc	Đáp ứng Mức 2 và có cơ chế cải tiến liên tục để tối ưu hoá giải pháp đảm bảo an ninh mạng cho hệ thống thư điện tử	Thuyết minh về giải pháp, tài liệu minh chứng.

					phương án tương đương.	hoặc phương án tương đương.	
		II.9.1.4. Đảm bảo phiên bản trình duyệt web và dịch vụ thư điện tử được rà soát, cập nhật bản vá lỗ hổng bảo mật	Chưa đáp ứng Mức 1.	Đã thực hiện kiểm tra để đảm bảo phiên bản trình duyệt web và dịch vụ thư điện tử được rà soát, cập nhật bản vá lỗ hổng bảo mật thường xuyên hoặc có biện pháp kiểm soát rủi ro tương đương.	Đáp ứng Mức 1 và có cơ chế đo lường, đánh giá tính hiệu quả của hoạt động đảm bảo phiên bản trình duyệt web và dịch vụ thư điện tử được rà soát, cập nhật bản vá lỗ hổng bảo mật.	Đáp ứng Mức 2 và có cơ chế cải tiến liên tục để tối ưu hoá hoạt động đảm bảo phiên bản trình duyệt web và dịch vụ thư điện tử được rà soát, cập nhật bản vá lỗ hổng bảo mật.	Kế hoạch rà soát, cập nhật bản vá lỗ hổng, tài liệu minh chứng.
	II.9.2. Sử dụng dịch vụ lọc tên miền	II.9.2.1. Triển khai sử dụng dịch vụ lọc tên miền trong cơ quan, tổ chức để ngăn chặn các tên miền giả mạo và độc hại	Chưa đáp ứng Mức 1.	Đã triển khai sử dụng dịch vụ lọc tên miền (DNS Filtering) trong cơ quan, tổ chức để ngăn chặn các tên miền giả mạo và độc hại.	Đáp ứng Mức 1 và có cơ chế đo lường, đánh giá tính hiệu quả của hoạt động triển khai sử dụng dịch vụ lọc tên miền.	Đáp ứng Mức 2 và có cơ chế cải tiến liên tục để tối ưu hoá hoạt động triển khai sử dụng dịch vụ lọc tên miền.	Danh sách tên miền độc hại cần được ngăn chặn bằng DNS Filtering, tài liệu minh chứng.
	II.9.3. Thực thi, cập nhật các bộ lọc URL và giới hạn số lượng kết nối đến các ứng dụng, dịch vụ (áp dụng đối với hệ thống thông tin cấp độ 4 trở lên)	II.9.3.1. Triển khai và định kỳ cập nhật các bộ lọc URL để hạn chế tài sản kết nối với các trang web độc hại tiềm ẩn hoặc không được chấp thuận	Chưa đáp ứng Mức 1.	Đã triển khai và định kỳ cập nhật các bộ lọc URL để hạn chế tài sản kết nối với các trang web độc hại tiềm ẩn hoặc không được chấp thuận.	Đáp ứng Mức 1 và có cơ chế đo lường, đánh giá tính hiệu quả của hoạt động triển khai và định kỳ cập nhật các bộ lọc URL để hạn chế tài sản kết nối với các trang web độc hại tiềm ẩn hoặc không được chấp thuận.	Đáp ứng Mức 2 và có cơ chế cải tiến liên tục để tối ưu hoá hoạt động triển khai và định kỳ cập nhật các bộ lọc URL để hạn chế tài sản kết nối với các trang web độc hại tiềm ẩn hoặc không được chấp thuận.	Danh sách URL cần được ngăn chặn
	II.9.4. Kiểm soát việc sử dụng các tiện ích mở rộng	II.9.4.1. Xác định danh sách tiện ích mở rộng được phép sử dụng	Chưa đáp ứng Mức 1.	Đã xác định danh sách tiện ích mở rộng được phép sử dụng trong trình duyệt web, dịch vụ thư điện tử.	Đáp ứng Mức 1 và có cơ chế đo lường, đánh giá tính hiệu quả của hoạt động xác định danh sách	Đáp ứng Mức 2 và có cơ chế cải tiến liên tục để tối ưu hoá hoạt động xác định danh sách tiện ích mở rộng	Danh sách tiện ích mở rộng được phép sử dụng trong trình duyệt

	trong trình duyệt web và dịch vụ thư điện tử (áp dụng đối với hệ thống thông tin cấp độ 4 trở lên)	trong trình duyệt web, dịch vụ thư điện tử.			tiện ích mở rộng được phép sử dụng trong trình duyệt web, dịch vụ thư điện tử.	được phép sử dụng trong trình duyệt web, dịch vụ thư điện tử.	web, dịch vụ thư điện tử
		II.9.4.2. Kiểm soát việc cài đặt và sử dụng các tiện ích mở rộng trong trình duyệt web, dịch vụ thư điện tử.	Chưa đáp ứng Mức 1.	Đã kiểm soát việc cài đặt và sử dụng các tiện ích mở rộng trong trình duyệt web, dịch vụ thư điện tử.	Đáp ứng Mức 1 và có cơ chế đo lường, đánh giá tính hiệu quả của hoạt động kiểm soát việc cài đặt và sử dụng các tiện ích mở rộng trong trình duyệt web, dịch vụ thư điện tử.	Đáp ứng Mức 2 và có cơ chế cải tiến liên tục để tối ưu hoá hoạt động kiểm soát việc cài đặt và sử dụng các tiện ích mở rộng trong trình duyệt web, dịch vụ thư điện tử.	Biện pháp kiểm sóat cài đặt và sử dụng các tiện ích mở rộng
		II.9.4.3. Gỡ cài đặt hoặc vô hiệu hóa các tiện ích mở rộng không được cấp phép.	Chưa đáp ứng Mức 1.	Đã gỡ cài đặt hoặc vô hiệu hóa các tiện ích mở rộng không được cấp phép.	Đáp ứng Mức 1 và có cơ chế đo lường, đánh giá tính hiệu quả của hoạt động gỡ cài đặt hoặc vô hiệu hóa các tiện ích mở rộng không được cấp phép.	Đáp ứng Mức 2 và có cơ chế cải tiến liên tục để tối ưu hoá hoạt động gỡ cài đặt hoặc vô hiệu hóa các tiện ích mở rộng không được cấp phép.	Quy định gỡ hoặc vô hiệu hóa các tiện ích mở rộng không được cấp phép
	II.9.5. Triển khai giải pháp xác thực email (áp dụng đối với hệ thống thông tin cấp độ 4 trở lên)	II.9.5.1. Triển khai giải pháp xác thực email	Chưa đáp ứng Mức 1.	Đã triển khai giải pháp xác thực email thông qua DMARC để tăng cường bảo mật và ngăn chặn các cuộc tấn công lừa đảo, giả mạo đối với các tên miền của tổ chức.	Đáp ứng Mức 1 và có cơ chế đo lường, đánh giá tính hiệu quả của hoạt động triển khai giải pháp xác thực email thông qua DMARC để tăng cường bảo mật và ngăn chặn các cuộc tấn công lừa đảo, giả mạo đối với các tên miền của tổ chức.	Đáp ứng Mức 2 và có cơ chế cải tiến liên tục để tối ưu hoá hoạt động triển khai giải pháp xác thực email thông qua DMARC để tăng cường bảo mật và ngăn chặn các cuộc tấn công lừa đảo, giả mạo đối với các tên miền của tổ chức.	Quy trình triển khai DMARC
	II.9.6. Quản lý các loại tệp được phép đính kèm trong thư	II.9.6.1. Xác định danh sách các loại tệp được phép gửi	Chưa đáp ứng Mức 1.	Đã xác định danh sách các loại tệp được phép gửi qua hệ thống thư điện tử.	Đáp ứng Mức 1 và có cơ chế đo lường, đánh giá tính hiệu quả của hoạt động xác định	Đáp ứng Mức 2 và có cơ chế cải tiến liên tục để tối ưu hoá hoạt động xác định danh	Danh sách các loại tệp được phép gửi qua hệ thống

	điện tử (áp dụng đối với hệ thống thông tin cấp độ 4 trở lên)	qua hệ thống thư điện tử			danh sách các loại tệp được phép gửi qua hệ thống thư điện tử.	sách các loại tệp được phép gửi qua hệ thống thư điện tử.	
		II.9.6.2. Ngăn chặn việc đính kèm những loại tệp không có trong danh sách cho phép và kiểm soát thư điện tử có chứa tệp đính kèm	Chưa đáp ứng Mức 1.	Đã ngăn chặn việc đính kèm những loại tệp không có trong danh sách cho phép và kiểm soát thư điện tử có chứa tệp đính kèm.	Đáp ứng Mức 1 và có cơ chế đo lường, đánh giá tính hiệu quả của hoạt động ngăn chặn việc đính kèm những loại tệp không có trong danh sách cho phép và kiểm soát thư điện tử có chứa tệp đính kèm.	Đáp ứng Mức 2 và có cơ chế cải tiến liên tục để tối ưu hoá hoạt động ngăn chặn việc đính kèm những loại tệp không có trong danh sách cho phép và kiểm soát thư điện tử có chứa tệp đính kèm.	Biện pháp ngăn chặn các loại tệp không có trong danh sách và kiểm soát thư điện tử có chứa tệp đính kèm
	II.9.7. Triển khai và duy trì biện pháp bảo vệ mã độc đối với máy chủ thư điện tử (áp dụng đối với hệ thống thông tin cấp độ 5)	II.9.7.1. Xây dựng và triển khai các phương án bảo vệ mã độc đối với máy chủ thư điện tử	Chưa đáp ứng Mức 1.	Đã triển khai các phương án bảo vệ mã độc đối với máy chủ thư điện tử.	Đáp ứng Mức 1 và có cơ chế đo lường, đánh giá tính hiệu quả của hoạt động xây dựng và triển khai các phương án bảo vệ mã độc đối với máy chủ thư điện tử.	Đáp ứng Mức 2 và có cơ chế cải tiến liên tục để tối ưu hoá hoạt động xây dựng và triển khai các phương án bảo vệ mã độc đối với máy chủ thư điện tử.	Phương án bảo vệ mã độc đối với máy chủ thư điện tử
II.10. Phòng chống phần mềm độc hại	II.10.1. Triển khai và duy trì phần mềm, giải pháp phòng chống mã độc	II.10.1.1. Triển khai và duy trì phần mềm, giải pháp phòng, chống mã độc trên máy chủ, máy tính người dùng	Chưa đáp ứng Mức 1.	Đã triển khai và duy trì phần mềm, giải pháp phòng, chống mã độc trên máy chủ, máy tính người dùng.	Đáp ứng Mức 1 và có cơ chế đo lường, đánh giá tính hiệu quả của hoạt động triển khai và duy trì phần mềm, giải pháp phòng, chống mã độc trên máy chủ, máy tính người dùng.	Đáp ứng Mức 2 và có cơ chế cải tiến liên tục để tối ưu hoá hoạt động triển khai và duy trì phần mềm, giải pháp phòng, chống mã độc trên máy chủ, máy tính người dùng.	Kết quả thực hiện rà quét mã độc
		II.10.1.2. Các tính năng cơ bản của giải	Chưa đáp ứng Mức 1.	Đã sử dụng giải pháp phòng, chống mã độc với các tính năng cơ bản như	Đáp ứng Mức 1 và có cơ chế đo lường, đánh giá tính hiệu	Đáp ứng Mức 2 và có cơ chế cải tiến liên tục để tối ưu hoá hoạt	Các giải pháp phòng chống mã độc

		pháp phòng, chống mã độc		bảo vệ thời gian thực, phát hiện mã độc dựa trên hành vi và tự động cập nhật mẫu nhận diện mã độc mới.	quả của hoạt động sử dụng giải pháp phòng, chống mã độc với các tính năng cơ bản như bảo vệ thời gian thực và tự động cập nhật mẫu nhận diện mã độc mới.	động sử dụng giải pháp phòng, chống mã độc với các tính năng cơ bản như bảo vệ thời gian thực và tự động cập nhật mẫu nhận diện mã độc mới.	
	II.10.2. Thực hiện phòng, chống mã độc đối với các thiết bị lưu trữ ngoài	II.10.2.1. Triển khai rà quét mã độc và vô hiệu hoá tính năng tự động thực thi đối với các phương tiện lưu trữ di động	Chưa đáp ứng Mức 1.	Đã triển khai rà quét mã độc và vô hiệu hoá tính năng tự động thực thi (autorun, autoplay…) đối với các phương tiện lưu trữ di động như ổ cứng, thẻ nhớ, USB…	Đáp ứng Mức 1 và có cơ chế đo lường, đánh giá tính hiệu quả của hoạt động rà quét mã độc và vô hiệu hoá tính năng tự động thực thi đối với các phương tiện lưu trữ di động như ổ cứng, thẻ nhớ, USB…	Đáp ứng Mức 2 và có cơ chế cải tiến liên tục để tối ưu hoá hoạt động rà quét mã độc và vô hiệu hoá tính năng tự động thực thi đối với các phương tiện lưu trữ di động như ổ cứng, thẻ nhớ, USB…	Kết quả thực hiện rà quét mã độc đối với các phương tiện lưu trữ di động
	II.10.3. Quản lý tập trung các phần mềm phòng, chống mã độc (áp dụng đối với hệ thống thông tin cấp độ 4 trở lên)	II.10.3.1. Quản lý tập trung các phần mềm phòng, chống mã độc	Chưa đáp ứng Mức 1.	Quản lý tập trung (cập nhật, cảnh báo và quản lý) các phần mềm phòng chống mã độc cài đặt trên máy chủ và các máy tính người sử dụng trong hệ thống.	Đáp ứng Mức 1 và có cơ chế đo lường, đánh giá tính hiệu quả của hoạt động quản lý tập trung.	Đáp ứng Mức 2 và có cơ chế cải tiến liên tục để tối ưu hoá hoạt động quản lý tập trung.	Kết quả thực hiện, tài liệu minh chứng.
	II.10.4. Kích hoạt tính năng phòng chống khai thác lỗ hổng	II.10.4.1. Kích hoạt tính năng phòng chống khai thác lỗ hổng trên các tài sản phần cứng và phần mềm (nếu có)	Chưa đáp ứng Mức 1.	Đã kích hoạt tính năng phòng chống khai thác lỗ hổng trên các tài sản phần cứng và phần mềm.	Đáp ứng Mức 1 và có cơ chế đo lường, đánh giá tính hiệu quả của hoạt động kích hoạt tính năng phòng chống khai thác lỗ hổng trên các	Đáp ứng Mức 2 và có cơ chế cải tiến liên tục để tối ưu hoá hoạt động kích hoạt tính năng phòng chống khai thác lỗ hổng trên các tài sản phần cứng và phần mềm.	Tài liệu minh chứng cho tính năng phòng chống khai thác lỗ hổng.

					tài sản phần cứng và phần mềm.		
	II.10.5. Xây dựng và triển khai giải pháp phòng chống mã độc theo hành vi	II.10.5.1. Triển khai giải pháp EDR hoặc phương án tương đương	Chưa đáp ứng Mức 1.	Đã triển khai giải pháp EDR hoặc phương án tương đương có khả năng phát hiện mã độc, mối nguy dựa trên hành vi trên máy chủ, máy tính người dùng.	Đáp ứng Mức 1 và có cơ chế đo lường, đánh giá tính hiệu quả của hoạt động triển khai giải pháp EDR hoặc phương án tương đương.	Đáp ứng Mức 2 và có cơ chế cải tiến liên tục để tối ưu hoá hoạt động triển khai giải pháp EDR hoặc phương án tương đương.	Thuyết minh, tài liệu minh chứng.
		II.10.5.2. Kết nối về SIEM	Chưa đáp ứng Mức 1.	Đã kết nối về SIEM để thực hiện giám sát theo thời gian thực và đưa ra cảnh báo.	Đáp ứng Mức 1 và có cơ chế đo lường, đánh giá tính hiệu quả của hoạt động kết nối về SIEM để thực hiện giám sát theo thời gian thực và đưa ra cảnh báo.	Đáp ứng Mức 2 và có cơ chế cải tiến liên tục để tối ưu hoá hoạt động kết nối về SIEM để thực hiện giám sát theo thời gian thực và đưa ra cảnh báo.	Báo cáo, tài liệu chứng minh.
II.11. Sao lưu và khôi phục dữ liệu	II.11.1. Xây dựng và tuân thủ quy định sao lưu, khôi phục dữ liệu	II.11.1.1. Xây dựng, ban hành, đảm bảo tuân thủ quy định sao lưu và khôi phục dữ liệu	Chưa đáp ứng Mức 1.	Đáp ứng tất cả các yêu cầu sau: - Đã ban hành quy định sao lưu và khôi phục dữ liệu, tối thiểu bao gồm: + Định nghĩa các loại dữ liệu cần được sao lưu và khôi phục cơ bản sau: tập tin cấu hình hệ thống, bản dự phòng hệ điều hành máy chủ, cơ sở dữ liệu, dữ liệu, thông tin nghiệp vụ; + Xác định tần suất sao lưu và khôi phục tương ứng với từng loại dữ liệu đã định nghĩa;	Đáp ứng Mức 1 và có cơ chế đo lường, đánh giá tính hiệu quả của việc thực hiện quy định sao lưu và khôi phục dữ liệu.	Đáp ứng Mức 2 và có cơ chế cải tiến liên tục để tối ưu hoá quy định sao lưu và khôi phục dữ liệu.	Quy định sao lưu và khôi phục dữ liệu

				+ Xác định phương pháp sao lưu và khôi phục tương ứng với từng loại dữ liệu đã định nghĩa; + Quản lý vùng lưu trữ dữ liệu sao lưu, đảm bảo tính toàn vẹn của dữ liệu và khôi phục dữ liệu một cách nhanh, hiệu quả; + Định kỳ thực hiện khôi phục dữ liệu đã sao lưu dựa trên mức độ nhạy cảm và tầm quan trọng của dữ liệu nhằm kiểm tra khả năng khôi phục của bản sao lưu; - Có cơ chế đảm bảo tuân thủ quy định.			
		II.11.1.2. Sử dụng giải pháp quản lý lưu trữ tập trung	Chưa đáp ứng Mức 1.	Đã sử dụng giải pháp quản lý lưu trữ tập trung hoặc có phương án sao lưu dự phòng tập trung đảm bảo tính sẵn sàng, cho phép khôi phục dữ liệu khi một thành phần trong hệ thống xảy ra sự cố.	Đáp ứng Mức 1 và có cơ chế đo lường, đánh giá tính hiệu quả của giải pháp quản lý lưu trữ tập trung hoặc phương án sao lưu dự phòng tập trung.	Đáp ứng Mức 2 và có cơ chế cải tiến liên tục để tối ưu hoá giải pháp quản lý lưu trữ tập trung hoặc phương án sao lưu dự phòng tập trung.	Thuyết minh, tài liệu minh chứng.
		II.11.1.3. Rà soát và cập nhật quy định sao lưu và khôi phục dữ liệu	Chưa đáp ứng Mức 3.			Đã thực hiện rà soát và cập nhật quy định tối thiểu 01 lần/năm hoặc khi xảy thay đổi trong tổ chức ảnh hưởng đến quy định.	Kết quả cập nhật quy trình
		II.11.2.1. Xác định danh sách	Chưa đáp ứng Mức 1.	Đã xác định danh sách dữ liệu cần sao lưu và phân	Đáp ứng Mức 1 và có cơ chế đo lường,	Đáp ứng Mức 2 và có cơ chế cải tiến liên	Danh sách dữ liệu cần sao lưu

	II.11.2. Thực hiện sao lưu dữ liệu tự động	dữ liệu cần sao lưu và phân loại tần suất sao lưu theo thời gian đối với từng loại dữ liệu		loại tần suất sao lưu theo thời gian (ngày/tuần/tháng/năm…) đối với từng loại dữ liệu.	đánh giá tính hiệu quả của hoạt động xác định danh sách dữ liệu cần sao lưu và phân loại tần suất sao lưu theo thời gian đối với từng loại dữ liệu.	tục để tối ưu hoá hoạt động xác định danh sách dữ liệu cần sao lưu và phân loại tần suất sao lưu theo thời gian đối với từng loại dữ liệu.	và phân loại tần suất sao lưu
		II.11.2.2. Triển khai các giải pháp sao lưu dữ liệu tự động	Chưa đáp ứng Mức 1.	Đã triển khai các giải pháp hoặc có biện pháp tương đương đảm bảo sao lưu dữ liệu tự động.	Đáp ứng Mức 1 và có cơ chế đo lường, đánh giá tính hiệu quả của hoạt động triển khai các giải pháp sao lưu dữ liệu tự động.	Đáp ứng Mức 2 và có cơ chế cải tiến liên tục để tối ưu hoá hoạt động triển khai các giải pháp sao lưu dữ liệu tự động.	Kế hoạch triển khai hoặc tập luật sao lưu dữ liệu tự động
	II.11.3. Bảo vệ bản sao lưu dữ liệu	II.11.3.1. Thực hiện bảo vệ bản sao lưu dữ liệu đảm bảo tính toàn vẹn, tính sẵn sàng và khả năng khôi phục của dữ liệu	Chưa đáp ứng Mức 1.	Đã áp dụng quy tắc sao lưu 3-2-1 hoặc có biện pháp tương đương bảo vệ bản sao lưu dữ liệu đảm bảo tính toàn vẹn, tính sẵn sàng và khả năng khôi phục của dữ liệu.	Đáp ứng Mức 1 và có cơ chế đo lường, đánh giá tính hiệu quả của hoạt động bảo vệ bản sao lưu dữ liệu nhằm đảm bảo tính toàn vẹn, tính sẵn sàng và khả năng khôi phục của dữ liệu.	Đáp ứng Mức 2 và có cơ chế cải tiến liên tục để tối ưu hoá hoạt động bảo vệ bản sao lưu dữ liệu nhằm đảm bảo tính toàn vẹn, tính sẵn sàng và khả năng khôi phục của dữ liệu.	Phương án bảo vệ bản sao lưu dữ liệu.
		II.11.3.2. Thực hiện mã hoá đối với những bản sao lưu dữ liệu quan trọng	Chưa đáp ứng Mức 1.	Đã thực hiện mã hoá đối với những bản sao lưu dữ liệu quan trọng.	Đáp ứng Mức 1 và có cơ chế đo lường, đánh giá tính hiệu quả của hoạt động mã hoá đối với những bản sao lưu dữ liệu quan trọng.	Đáp ứng Mức 2 và có cơ chế cải tiến liên tục để tối ưu hoá hoạt động mã hoá đối với những bản sao lưu dữ liệu quan trọng.	Phương pháp mã hóa bản sao lưu dữ liệu quan trọng
	II.11.4. Thiết lập và duy trì hạ tầng lưu trữ tách biệt cho bản sao lưu dữ liệu	II.11.4.1. Các bản sao lưu dữ liệu được định danh, quản lý phiên bản và lưu trữ ở những hạ tầng tách	Chưa đáp ứng Mức 1.	Đã thực hiện định danh, quản lý phiên bản và lưu trữ các bản sao lưu dữ liệu tại hạ tầng tách biệt với môi trường vận hành.	Đáp ứng Mức 1 và có cơ chế đo lường, đánh giá tính hiệu quả của hoạt động định danh, quản lý phiên bản và lưu trữ các bản sao lưu dữ	Đáp ứng Mức 2 và có cơ chế cải tiến liên tục để tối ưu hoá hoạt động định danh, quản lý phiên bản và lưu trữ các bản sao lưu dữ liệu tại hạ tầng	Giải pháp lưu trữ tách biệt

		biệt với môi trường vận hành			liệu tại hạ tầng tách biệt với môi trường vận hành.	tách biệt với môi trường vận hành.	
		II.11.4.2. Lưu trữ dự phòng ở vị trí địa lý khác nhau (áp dụng đối với hệ thống thông tin cấp độ 5)	Chưa đáp ứng Mức 1.	Lưu trữ dự phòng các dữ liệu quan trọng, dữ liệu có độ nhạy cảm cao trên hệ thống/phương tiện lưu trữ dự phòng ở vị trí địa lý khác nhau; bảo đảm môi trường bảo quản và phương pháp quản lý giống như với hệ thống chính.	Đáp ứng Mức 1 và có cơ chế đo lường, đánh giá tính hiệu quả của hoạt động lưu trữ dự phòng ở vị trí địa lý khác nhau.	Đáp ứng Mức 2 và có cơ chế cải tiến liên tục để tối ưu hoá hoạt động lưu trữ dự phòng ở vị trí địa lý khác nhau.	Thuyết minh, tài liệu minh chứng.
		II.11.4.3. Duy trì kết nối mạng giữa các hệ thống sao lưu dự phòng (áp dụng đối với hệ thống thông tin cấp độ 5)	Chưa đáp ứng Mức 1.	Duy trì ít nhất 02 kết nối mạng từ hệ thống sao lưu dự phòng chính với hệ thống sao lưu dự phòng phụ.	Đáp ứng Mức 1 và có cơ chế đo lường, đánh giá tính hiệu quả của hoạt động duy trì kết nối mạng giữa các hệ thống sao lưu dự phòng.	Đáp ứng Mức 2 và có cơ chế cải tiến liên tục để tối ưu hoá hoạt động duy trì kết nối mạng giữa các hệ thống sao lưu dự phòng.	Thuyết minh, tài liệu minh chứng.
	II.11.5. Kiểm tra khả năng khôi phục dữ liệu (áp dụng đối với hệ thống thông tin cấp độ 4 trở lên)	II.11.5.1. Phương án khôi phục tính nguyên vẹn của dữ liệu	Chưa đáp ứng Mức 1.	Có phương án khôi phục tính nguyên vẹn của dữ liệu. Kiểm tra khả năng khôi phục bản sao lưu dữ liệu, trong đó: - Cấp độ 4: tối thiểu 01 lần/06 tháng; - Cấp độ 5: tối thiểu 01 lần/01 quý.	Đáp ứng Mức 1 và có cơ chế đo lường, đánh giá tính hiệu quả của hoạt động	Đáp ứng Mức 2 và có cơ chế cải tiến liên tục để tối ưu hoá hoạt động	Thuyết minh, tài liệu minh chứng.
II.12. Quản lý hạ tầng mạng	II.12.1. Thiết lập, duy trì các sơ đồ kiến trúc hệ thống mạng	II.12.1.1. Thiết lập và duy trì sơ đồ kiến trúc mạng và các hồ	Chưa đáp ứng Mức 1.	Đã thiết lập và duy trì sơ đồ kiến trúc mạng và các hồ sơ khác về hệ thống mạng. Đối với hệ thống thông tin cấp độ 4 trở lên,	Đáp ứng Mức 1 và có cơ chế đo lường, đánh giá tính hiệu quả của hoạt động thiết lập và duy trì sơ	Đáp ứng Mức 2 và có cơ chế cải tiến liên tục để tối ưu hoá hoạt động thiết lập và duy trì sơ đồ kiến trúc	Sơ đồ kiến trúc mạng và các hồ sơ khác về hệ thống mạng

	và kiến trúc mạng an toàn	sơ khác về hệ thống mạng		có bộ phận chuyên môn, tổ chức chuyên gia đánh giá hồ sơ thiết kế hệ thống thông tin, các biện pháp đảm bảo an ninh mạng trước khi triển khai thực hiện.	đồ kiến trúc mạng và các hồ sơ khác về hệ thống mạng	mạng và các hồ sơ khác về hệ thống mạng.	
		II.12.1.2. Thiết kế theo nguyên tắc Zero trust (áp dụng đối với hệ thống thông tin cấp độ 4 trở lên)	Chưa đáp ứng Mức 1.	Thiết kế kiến trúc hệ thống mạng theo nguyên tắc Zero trust, lấy tài nguyên/dữ liệu làm trung tâm bảo vệ, áp dụng phân đoạn vi mô để cách ly các máy chủ, ứng dụng quan trọng.	Đáp ứng Mức 1 và có cơ chế đo lường, đánh giá tính hiệu quả của hoạt động thiết kế theo nguyên tắc Zero trust.	Đáp ứng Mức 2 và có cơ chế cải tiến liên tục để tối ưu hoá hoạt động thiết kế theo nguyên tắc Zero trust.	Sơ đồ, tài liệu minh chứng.
		II.12.1.3. Triển khai và duy trì một kiến trúc hệ thống mạng an toàn	Chưa đáp ứng Mức 1.	Đã triển khai và duy trì kiến trúc hệ thống mạng an toàn theo 03 nguyên tắc: phân vùng mạng, đặc quyền ít nhất và tính sẵn sàng.	Đáp ứng Mức 1 và có cơ chế đo lường, đánh giá tính hiệu quả của hoạt động triển khai và duy trì kiến trúc hệ thống mạng an toàn theo 03 nguyên tắc: phân vùng mạng, đặc quyền ít nhất và tính sẵn sàng.	Đáp ứng Mức 2 và có cơ chế cải tiến liên tục để tối ưu hoá hoạt động triển khai và duy trì kiến trúc hệ thống mạng an toàn theo 03 nguyên tắc: phân vùng mạng, đặc quyền ít nhất và tính sẵn sàng.	Kiến trúc hệ thống mạng an toàn, đảm bảo thực hiện tối thiểu 03 nguyên tắc: phân vùng mạng, đặc quyền ít nhất và tính sẵn sàng
		II.12.1.4. Triển khai kết nối mạng an toàn (áp dụng đối với hệ thống thông tin cấp độ 4 trở lên)	Chưa đáp ứng Mức 1.	Triển khai kết nối mạng an toàn, bảo đảm an toàn trong quá trình khởi tạo kết nối kênh truyền và trao đổi thông tin qua kênh truyền.	Đáp ứng Mức 1 và có cơ chế đo lường, đánh giá tính hiệu quả của hoạt động triển khai kết nối mạng an toàn.	Đáp ứng Mức 2 và có cơ chế cải tiến liên tục để tối ưu hoá hoạt động triển khai kết nối mạng an toàn.	Sơ đồ, tài liệu minh chứng.
		II.12.1.5. Tài liệu hóa sơ đồ	Chưa đáp ứng Mức 1.	Đã tài liệu hóa sơ đồ kiến trúc hệ thống mạng, tối thiểu bao gồm:	Đáp ứng Mức 1 và có cơ chế đo lường, đánh giá tính hiệu	Đáp ứng Mức 2 và có cơ chế cải tiến liên tục để tối ưu hoá hoạt	Sơ đồ, tài liệu mô tả chi tiết

		kiến trúc hệ thống mạng		- Tổng quan kiến trúc hệ thống mạng; - Sơ đồ cấp chi tiết của hệ thống mạng; - Ghi chú các tài liệu đặc tả kỹ thuật, tài liệu thống kê…; - Tài liệu mô tả phương án đảm bảo an ninh mạng.	quả của hoạt động tài liệu hóa sơ đồ kiến trúc hệ thống mạng.	động tài liệu hóa sơ đồ kiến trúc hệ thống mạng.	kiến trúc hệ thống mạng
		II.12.1.6. Quản lý và bảo vệ tài liệu, hồ sơ thiết kế (áp dụng đối với hệ thống thông tin cấp độ 4 trở lên)	Chưa đáp ứng Mức 1.	Xây dựng phương án và thực hiện quản lý và bảo vệ tài liệu, hồ sơ thiết kế.	Đáp ứng Mức 1 và có cơ chế đo lường, đánh giá tính hiệu quả của hoạt động quản lý và bảo vệ tài liệu, hồ sơ thiết kế.	Đáp ứng Mức 2 và có cơ chế cải tiến liên tục để tối ưu hoá hoạt động quản lý và bảo vệ tài liệu, hồ sơ thiết kế.	Sơ đồ, tài liệu minh chứng.
		II.12.1.7. Đánh giá lại tính phù hợp của phương án thiết kế	Chưa đáp ứng Mức 1.	Khi có thay đổi thiết kế, đánh giá lại tính phù hợp của phương án thiết kế đối với các yêu cầu an toàn đặt ra đối với hệ thống.	Đáp ứng Mức 1 và có cơ chế đo lường, đánh giá tính hiệu quả của hoạt động đánh giá lại tính phù hợp của phương án thiết kế.	Đáp ứng Mức 2 và có cơ chế cải tiến liên tục để tối ưu hoá hoạt động đánh giá lại tính phù hợp của phương án thiết kế.	Bản đánh giá lại tính phù hợp, tài liệu minh chứng.
		II.12.1.8. Xem xét và cập nhật sơ đồ mạng	Chưa đáp ứng Mức 3.			Đã xem xét và cập nhật sơ đồ mạng định kỳ hoặc mỗi khi có thay đổi ảnh hưởng đến sơ đồ hệ thống, trong đó: - Cấp độ 3: tối thiểu 01 lần/01 năm; - Cấp độ 4: tối thiểu 01 lần/06 tháng; - Cấp độ 5: tối thiểu 01 lần/01 quý.	Bản cập nhật sơ đồ mạng.

	II.12.2. Quản lý an toàn cơ sở hạ tầng mạng	II.12.2.1. Thực hiện quản lý an toàn cơ sở hạ tầng mạng	Chưa đáp ứng Mức 1.	- Đã thực hiện quản lý an toàn cơ sở hạ tầng mạng, đảm bảo tối thiểu: + Có phương án cân bằng tải và dự phòng nóng cho các thiết bị mạng chính. + Có phương án phòng, chống thất thoát dữ liệu. + Có phương án dự phòng kết nối mạng cho các máy chủ cung cấp dịch vụ. + Sử dụng giải pháp tường lửa có tích hợp chức năng phòng, chống xâm nhập hoặc có phương án tương đương phục vụ kiểm soát truy cập, phòng, chống xâm nhập giữa các vùng mạng. + Sử dụng giải pháp tường lửa tích hợp chức năng phòng, chống mã độc trên môi trường mạng hoặc có phương án tương đương. + Sử dụng giải pháp DBF hoặc có phương án tương đương đối với hệ thống cơ sở dữ liệu tập trung. + Sử dụng giải pháp quản lý truy cập lớp mạng hoặc có phương án tương đương kiểm soát truy cập lớp mạng, kiểm soát truy cập thiết bị đầu cuối, máy	Đáp ứng Mức 1 và có cơ chế đo lường, đánh giá tính hiệu quả của hoạt động quản lý an toàn cơ sở hạ tầng mạng	Đáp ứng Mức 2 và có cơ chế cải tiến liên tục để tối ưu hoá hoạt động quản lý an toàn cơ sở hạ tầng mạng	Các phương án thực hiện quản lý an toàn cơ sở hạ tầng mạng, tài liệu minh chứng.

				tính người dùng kết nối vào mạng. + Có phương án giám sát hệ thống thông tin tập trung. + Sử dụng giải pháp WAF hoặc có phương án tương đương phục vụ phòng chống tấn công ứng dụng web (nếu có). + Sử dụng dịch vụ của doanh nghiệp hoặc sản phẩm phòng, chống tấn công từ chối dịch vụ hoặc có phương án tương đương phòng, chống tấn công từ chối dịch vụ. + Định kỳ cập nhật cơ sở dữ liệu phát hiện tấn công mạng cho các giải pháp đảm bảo an ninh mạng trong hệ thống thông tin. + Thực hiện quản lý thay đổi. + Kiểm tra hiệu năng (RAM, CPU...), đảm bảo hoạt động bình thường của hệ thống. - Đối với hệ thống thông tin cấp độ 4 trở lên: + Đối với các hệ thống có kết nối mạng Internet, đã xây dựng và triển khai phương án duy trì ít nhất 02 hướng kết nối mạng			

				Internet quốc tế từ các nhà cung cấp dịch vụ trong nước có hạ tầng khác nhau. + Tách biệt, cô lập vật lý hoặc sử dụng Datadiode, USG, BSG hoặc có phương án kiểm soát rủi ro tương đương phân vùng, bảo mật, kiểm soát luồng dữ liệu cho vùng mạng lõi, vùng mạng OT với vùng mạng có mức độ tin cậy thấp hơn, bao gồm nhưng không giới hạn: vùng mạng có kết nối Internet, vùng mạng không dây công cộng/ dùng riêng và các mạng kết nối từ xa của bên thứ ba. - Đối với hệ thống thông tin cấp độ 5: + Có phương án dự phòng hệ thống ở vị trí địa lý khác nhau, cách nhau tối thiểu 30 km. + Có phương án dự phòng cho kết nối mạng giữa các hệ thống chính và dự phòng.			
		II.12.2.2. Chia tách thành các vùng mạng khác nhau theo đối tượng sử	Chưa đáp ứng Mức 1.	- Đã chia tách thành các vùng mạng khác nhau theo đối tượng và mục đích sử dụng, tối thiểu: Vùng mạng nội bộ; Vùng mạng biên; Vùng mạng	Đáp ứng Mức 1 và có cơ chế đo lường, đánh giá tính hiệu quả của hoạt động chia tách thành các vùng mạng khác	Đáp ứng Mức 2 và có cơ chế cải tiến liên tục để tối ưu hoá hoạt động chia tách thành các vùng mạng khác	Sơ đồ vùng mạng, tài liệu minh chứng.

		dụng, mục đích sử dụng		máy chủ nội bộ; Vùng mạng trung gian (DMZ) để cung cấp dịch vụ; Vùng mạng máy chủ cơ sở dữ liệu; Vùng mạng riêng để cung cấp dịch vụ mạng không dây (nếu có); Vùng quản trị. - Đối với với hệ thống thông tin cấp độ 4 trở lên: Vùng mạng WAN diện rộng; Vùng quản trị thiết bị hệ thống.	nhau theo đối tượng và mục đích sử dụng.	nhau theo đối tượng và mục đích sử dụng.	
	II.12.3. Kiểm thử và nghiệm thu hệ thống	II.12.3.1. Có nội dung, kế hoạch, quy trình thử nghiệm và nghiệm thu hệ thống	Chưa đáp ứng Mức 1.	Đã có nội dung, kế hoạch và quy trình thử nghiệm, nghiệm thu hệ thống.	Đáp ứng Mức 1 và có cơ chế đo lường, đánh giá tính hiệu quả của nội dung, kế hoạch và quy trình thử nghiệm, nghiệm thu hệ thống.	Đáp ứng Mức 2 và có cơ chế cải tiến liên tục để tối ưu hoá nội dung, kế hoạch và quy trình thử nghiệm, nghiệm thu hệ thống.	Quy trình thử nghiệm và nghiệm thu hệ thống
		II.12.3.2. Thực hiện kiểm thử hệ thống trước khi đưa vào vận hành, khai thác sử dụng	Chưa đáp ứng Mức 1.	Đã kiểm thử hệ thống trước khi đưa vào vận hành, khai thác sử dụng.	Đáp ứng Mức 1 và có cơ chế đo lường, đánh giá tính hiệu quả của hoạt động kiểm thử hệ thống trước khi đưa vào vận hành, khai thác sử dụng.	Đáp ứng Mức 2 và có cơ chế cải tiến liên tục để tối ưu hoá hoạt động kiểm thử hệ thống trước khi đưa vào vận hành, khai thác sử dụng.	Báo cáo kiểm thử trước khi đưa vào vận hành, khai thác sử dụng.
		II.12.3.3. Có bộ phận chịu trách nhiệm thực hiện thử nghiệm và nghiệm thu hệ thống	Chưa đáp ứng Mức 1.	Có bộ phận chịu trách nhiệm thực hiện thử nghiệm và nghiệm thu hệ thống.	Đáp ứng Mức 1 và có cơ chế đo lường, đánh giá tính hiệu quả của bộ phận chịu trách nhiệm thực hiện thử nghiệm và nghiệm thu hệ thống.	Đáp ứng Mức 2 và có cơ chế cải tiến liên tục để tối ưu hoá hoạt động của bộ phận chịu trách nhiệm thực hiện thử nghiệm	Biên bản, tài liệu minh chứng.

						và nghiệm thu hệ thống.	
		II.12.3.4. Có đơn vị độc lập hoặc bộ phận độc lập thuộc cơ quan, tổ chức thực hiện tư vấn và giám sát quá trình thử nghiệm và nghiệm thu hệ thống	Chưa đáp ứng Mức 1.	Đã có đơn vị độc lập (bên thứ ba) hoặc bộ phận độc lập thuộc cơ quan, tổ chức thực hiện tư vấn và giám sát quá trình thử nghiệm và nghiệm thu hệ thống.	Đáp ứng Mức 1 và có cơ chế đo lường, đánh giá tính hiệu quả của đơn vị độc lập hoặc bộ phận độc lập.	Đáp ứng Mức 2 và có cơ chế cải tiến liên tục để tối ưu hoá đơn vị độc lập hoặc bộ phận độc lập.	Danh sách đơn vị độc lập thực hiện tư vấn, giám sát quá trình thử nghiệm và nghiệm thu hệ thống.
		II.12.3.5. Có báo cáo nghiệm thu được xác nhận của bộ phận chuyên trách và phê duyệt của chủ quản hệ thống thông tin trước khi đưa vào sử dụng	Chưa đáp ứng Mức 1.	Có báo cáo nghiệm thu được xác nhận của bộ phận chuyên trách và phê duyệt của chủ quản hệ thống thông tin trước khi đưa vào sử dụng.	Đáp ứng Mức 1 và có cơ chế đo lường, đánh giá tính hiệu quả của hoạt động xác nhận, phê duyệt báo cáo nghiệm thu.	Đáp ứng Mức 2 và có cơ chế cải tiến liên tục để tối ưu hoá hoạt động xác nhận, phê duyệt báo cáo nghiệm thu.	Báo cáo nghiệm thu được xác nhận, phê duyệt, tài liệu minh chứng.
	II.12.4. Kiểm soát truy cập	II.12.4.1. Thiết lập hệ thống chỉ cho phép sử dụng các kết nối mạng an toàn khi truy cập thông tin nội bộ hoặc thực hiện quản trị từ xa đối với	Chưa đáp ứng Mức 1.	Đã thiết lập hệ thống chỉ cho phép sử dụng các kết nối mạng an toàn khi truy cập thông tin nội bộ hoặc thực hiện quản trị từ xa đối với tài sản phần cứng và phần mềm.	Đáp ứng Mức 1 và có cơ chế đo lường, đánh giá tính hiệu quả của hoạt động thiết lập hệ thống chỉ cho phép sử dụng các kết nối mạng an toàn khi truy cập thông tin nội bộ hoặc thực hiện quản trị từ xa đối với	Đáp ứng Mức 2 và có cơ chế cải tiến liên tục để tối ưu hoá hoạt động thiết lập hệ thống chỉ cho phép sử dụng các kết nối mạng an toàn khi truy cập thông tin nội bộ hoặc thực hiện quản trị từ xa đối với tài	Báo cáo, tài liệu chứng minh.

		tài sản phần cứng và phần mềm			tài sản phần cứng và phần mềm.	sản phần cứng và phần mềm.	
		II.12.4.2. Cấu hình chức năng xác thực trên các thiết bị hệ thống để xác thực người dùng khi quản trị thiết bị trực tiếp hoặc từ xa	Chưa đáp ứng Mức 1.	Đã cấu hình chức năng xác thực trên các thiết bị hệ thống để xác thực người dùng khi quản trị thiết bị trực tiếp hoặc từ xa.	Đáp ứng Mức 1 và có cơ chế đo lường, đánh giá tính hiệu quả của hoạt động cấu hình chức năng xác thực trên các thiết bị hệ thống để xác thực người dùng khi quản trị thiết bị trực tiếp hoặc từ xa.	Đáp ứng Mức 2 và có cơ chế cải tiến liên tục để tối ưu hoá hoạt động cấu hình chức năng xác thực trên các thiết bị hệ thống để xác thực người dùng khi quản trị thiết bị trực tiếp hoặc từ xa.	Báo cáo, tài liệu minh chứng.
		II.12.4.3. Thiết lập giới hạn thời gian chờ (timeout) để tự động đóng các phiên kết nối khi không nhận được yêu cầu từ người dùng trong một khoảng thời gian quy định	Chưa đáp ứng Mức 1.	Đã thiết lập giới hạn thời gian chờ (timeout) để tự động đóng các phiên kết nối khi không nhận được yêu cầu từ người dùng trong một khoảng thời gian quy định.	Đáp ứng Mức 1 và có cơ chế đo lường, đánh giá tính hiệu quả của hoạt động thiết lập giới hạn thời gian chờ.	Đáp ứng Mức 2 và có cơ chế cải tiến liên tục để tối ưu hoá hoạt động thiết lập giới hạn thời gian chờ.	Báo cáo, tài liệu minh chứng.
		II.12.4.4. Kiểm soát truy cập từ bên ngoài vào hệ thống và từ bên trong hệ thống ra ngoài theo từng dịch vụ, ứng dụng cụ thể	Chưa đáp ứng Mức 1.	Đã kiểm soát truy cập từ bên ngoài vào hệ thống và từ bên trong hệ thống ra ngoài theo từng dịch vụ, ứng dụng cụ thể; chặn tất cả truy cập tới các tài sản phần cứng và phần mềm mà hệ thống không cung cấp hoặc không cho phép truy cập.	Đáp ứng Mức 1 và có cơ chế đo lường, đánh giá tính hiệu quả của hoạt động kiểm soát truy cập từ bên ngoài vào hệ thống và từ bên trong hệ thống ra ngoài theo từng dịch vụ, ứng dụng cụ thể.	Đáp ứng Mức 2 và có cơ chế cải tiến liên tục để tối ưu hoá hoạt động kiểm soát truy cập từ bên ngoài vào hệ thống và từ bên trong hệ thống ra ngoài theo từng dịch vụ, ứng dụng cụ thể.	Báo cáo, tài liệu minh chứng.

		II.12.4.5. Giới hạn số lượng kết nối đồng thời	Chưa đáp ứng Mức 1.	Giới hạn số lượng kết nối đồng thời từ một địa chỉ nguồn và tổng số lượng kết nối đồng thời cho từng ứng dụng, dịch vụ được hệ thống cung cấp theo năng lực thực tế của hệ thống, không áp dụng cứng đối với hệ thống/dịch vụ có yêu cầu kết nối lớn nếu đã có biện pháp kiểm soát rủi ro tương đương.	Đáp ứng Mức 1 và có cơ chế đo lường, đánh giá tính hiệu quả của hoạt động giới hạn số lượng kết nối đồng thời.	Đáp ứng Mức 2 và có cơ chế cải tiến liên tục để tối ưu hoá hoạt động giới hạn số lượng kết nối đồng thời.	Báo cáo, tài liệu minh chứng.
		II.12.4.6. Phương án kiểm soát truy cập của người dùng vào các dịch vụ, các máy chủ nội bộ	Chưa đáp ứng Mức 1.	Có phương án kiểm soát truy cập của người dùng vào các dịch vụ, các máy chủ nội bộ theo chính sách.	Đáp ứng Mức 1 và có cơ chế đo lường, đánh giá tính hiệu quả của hoạt động kiểm soát truy cập của người dùng vào các dịch vụ, các máy chủ nội bộ.	Đáp ứng Mức 2 và có cơ chế cải tiến liên tục để tối ưu hoá hoạt động kiểm soát truy cập của người dùng vào các dịch vụ, các máy chủ nội bộ.	Báo cáo, tài liệu minh chứng.
		II.12.4.7. Giới hạn truy cập từ các máy chủ ra các mạng bên ngoài (áp dụng đối với hệ thống thông tin cấp độ 4 trở lên)	Chưa đáp ứng Mức 1.	Không cho phép hoặc giới hạn truy cập (theo chức năng của máy chủ) từ các máy chủ ra các mạng bên ngoài hệ thống.	Đáp ứng Mức 1 và có cơ chế đo lường, đánh giá tính hiệu quả của hoạt động giới hạn truy cập từ các máy chủ ra các mạng bên ngoài.	Đáp ứng Mức 2 và có cơ chế cải tiến liên tục để tối ưu hoá hoạt động giới hạn truy cập từ các máy chủ ra các mạng bên ngoài.	Tài liệu minh chứng.
		II.12.4.8. Bảo đảm chất lượng dịch vụ (áp dụng đối với hệ	Chưa đáp ứng Mức 1.	Có phương án ưu tiên, bảo đảm chất lượng dịch vụ (QoS).	Đáp ứng Mức 1 và có cơ chế đo lường, đánh giá tính hiệu quả của hoạt động	Đáp ứng Mức 2 và có cơ chế cải tiến liên tục để tối ưu hoá hoạt động bảo đảm chất lượng dịch vụ.	Tài liệu minh chứng.

		thống thông tin cấp độ 5)			bảo đảm chất lượng dịch vụ.		
	II.12.5. Xây dựng và áp dụng chính sách quản lý truy cập từ xa	II.12.5.1. Xây dựng và áp dụng chính sách quản lý truy cập từ xa	Chưa đáp ứng Mức 1.	Đã xây dựng và áp dụng chính sách quản lý truy cập từ xa đáp ứng các yêu cầu sau: - Sử dụng mạng riêng ảo VPN hoặc phương án tương đương và yêu cầu xác thực cho việc truy cập từ xa vào hệ thống đối với người dùng quản trị, người dùng tác nghiệp hệ thống; - Yêu cầu người dùng xác thực để kết nối truy cập từ xa và xác thực bổ sung trước khi truy cập vào hệ thống; đối với hệ thống thông tin cấp độ 4 trở lên, yêu cầu xác thực MFA. - Giới hạn các dải địa chỉ mạng hoặc thiết bị cụ thể (nếu hỗ trợ) được phép kết nối để thực hiện quản trị từ xa đối với tài sản phần cứng và phần mềm. - Đối với hệ thống thông tin cấp độ 4 trở lên, các thiết bị được phép truy cập từ xa đáp ứng các yêu cầu về bảo mật: đã cài đặt phần mềm phòng chống mã độc, cấu hình bảo mật theo chính sách an ninh,	Đáp ứng Mức 1 và có cơ chế đo lường, đánh giá tính hiệu quả của hoạt động xây dựng và áp dụng chính sách quản lý truy cập từ xa.	Đáp ứng Mức 2 và có cơ chế cải tiến liên tục để tối ưu hoá hoạt động xây dựng và áp dụng chính sách quản lý truy cập từ xa.	Chính sách quản lý truy cập từ xa, tài liệu minh chứng.

				an toàn đã ban hành của tổ chức.			
	II.12.6. Quản lý xác thực, cấp quyền và kiểm toán truy cập hệ thống thông tin (áp dụng đối với hệ thống thông tin cấp độ 5)	II.12.6.1. Giải pháp quản lý việc xác thực, cấp quyền và kiểm toán	Chưa đáp ứng Mức 1.	Có giải pháp quản lý việc xác thực, cấp quyền và kiểm toán truy cập hệ thống thông tin.	Đáp ứng Mức 1 và có cơ chế đo lường, đánh giá tính hiệu quả của hoạt động giải pháp quản lý việc xác thực, cấp quyền và kiểm toán.	Đáp ứng Mức 2 và có cơ chế cải tiến liên tục để tối ưu hoá hoạt động giải pháp quản lý việc xác thực, cấp quyền và kiểm toán.	Tài liệu minh chứng.
	II.12.7. Sử dụng các giao thức truyền thông và quản trị mạng an toàn (áp dụng đối với hệ thống thông tin cấp độ 4 trở lên)	II.12.7.1. Sử dụng các giao thức truyền thông và quản trị mạng an toàn	Chưa đáp ứng Mức 1.	Cấu hình hệ thống thông tin chỉ sử dụng các giao thức truyền thông và quản trị mạng an toàn (chưa được các tổ chức quốc tế công bố điểm yếu).	Đáp ứng Mức 1 và có cơ chế đo lường, đánh giá tính hiệu quả của hoạt động sử dụng các giao thức truyền thông và quản trị mạng an toàn	Đáp ứng Mức 2 và có cơ chế cải tiến liên tục để tối ưu hoá hoạt động sử dụng các giao thức truyền thông và quản trị mạng an toàn	Tài liệu minh chứng.
	II.12.8. Thiết lập và duy trì tài nguyên hệ thống dành riêng cho công tác quản trị (áp dụng đối với hệ thống thông tin cấp độ 4 trở lên)	II.12.8.1. Duy trì các nguồn tài nguyên dành riêng cho công tác quản trị	Chưa đáp ứng Mức 1.	Thiết lập và duy trì các nguồn tài nguyên dành riêng cho công tác quản trị, tách biệt về mặt vật lý hoặc logic; được phân tách với mạng chính của hệ thống và không kết nối với Internet.	Đáp ứng Mức 1 và có cơ chế đo lường, đánh giá tính hiệu quả của hoạt động duy trì các nguồn tài nguyên dành riêng cho công tác quản trị.	Đáp ứng Mức 2 và có cơ chế cải tiến liên tục để tối ưu hoá hoạt động duy trì các nguồn tài nguyên dành riêng cho công tác quản trị.	Tài liệu minh chứng.

II.13. Giám sát phòng thủ an ninh mạng (áp dụng đối với hệ thống thông tin cấp độ 4 trở lên)	II.13.1. Thực hiện giám sát và quản lý tập trung các cảnh báo và sự kiện an ninh mạng	II.13.1.1. Triển khai giám sát an ninh mạng	Chưa đáp ứng Mức 1.	Đã triển khai hoạt động giám sát an ninh mạng cho tối thiểu các đối tượng: thiết bị hệ thống, máy chủ, ứng dụng, dịch vụ và các thành phần khác trong hệ thống (nếu có).	Đáp ứng Mức 1 và có cơ chế đo lường, đánh giá tính hiệu quả của hoạt động giám sát an ninh mạng.	- Đáp ứng Mức 2 và có cơ chế cải tiến liên tục để tối ưu hóa hoạt động giám sát an ninh mạng.	Kế hoạch triển khai giám sát an ninh mạng tối thiểu đủ các đối tượng
		II.13.1.2. Triển khai SIEM	Chưa đáp ứng Mức 1.	Đã triển khai giải pháp quản lý nhật ký và sự kiện tập trung (SIEM) để liên kết các sự kiện liên quan, phân tích theo hướng dẫn, yêu cầu và quy định của cơ quan, tổ chức có thẩm quyền.	Đáp ứng Mức 1 và có cơ chế đo lường, đánh giá tính hiệu quả của hoạt động triển khai SIEM.	Đáp ứng Mức 2 và có cơ chế cải tiến liên tục để tối ưu hóa hoạt động triển khai SIEM.	Báo cáo, tài liệu minh chứng.
		II.13.1.3. Bố trí nguồn lực và tổ chức giám sát an ninh mạng 24/7	Chưa đáp ứng Mức 1.	Có bộ phận chịu trách nhiệm giám sát an ninh mạng 24/7; phân công rõ vai trò và thời gian trực.	Đáp ứng Mức 1 và có cơ chế đo lường, đánh giá tính hiệu quả của hoạt động bố trí nguồn lực và tổ chức giám sát an ninh mạng 24/7.	Đáp ứng Mức 2 và có cơ chế cải tiến liên tục để tối ưu hóa hoạt động bố trí nguồn lực và tổ chức giám sát an ninh mạng 24/7.	Danh sách bố trí nguồn lực, tổ chức giám sát an ninh mạng.
	II.13.2. Thiết lập và sử dụng tính năng về tường lửa, cảnh báo phát hiện và ngăn chặn xâm nhập của hệ điều hành và hệ thống	II.13.2.1. Thiết lập và sử dụng tính năng về tường lửa, cảnh báo phát hiện, ngăn chặn xâm nhập của hệ điều hành và hệ thống (nếu có)	Chưa đáp ứng Mức 1.	Đã thiết lập và sử dụng tính năng về tường lửa, cảnh báo phát hiện, ngăn chặn xâm nhập của hệ điều hành và hệ thống.	Đáp ứng Mức 1 và có cơ chế đo lường, đánh giá tính hiệu quả của hoạt động thiết lập và sử dụng tính năng về tường lửa, cảnh báo phát hiện, ngăn chặn xâm nhập của hệ điều hành và hệ thống.	Đáp ứng Mức 2 và có cơ chế cải tiến liên tục dựa trên kết quả đánh giá để tối ưu hóa hoạt động thiết lập và sử dụng tính năng về tường lửa, cảnh báo phát hiện, ngăn chặn xâm nhập của hệ điều hành và hệ thống.	Báo cáo, tài liệu minh chứng.

	II.13.3. Triển khai giải pháp, thiết bị chuyên dụng để bảo mật hệ thống mạng của cơ quan, tổ chức (áp dụng đối với hệ thống thông tin cấp độ 5)	II.13.3.1. Triển khai các giải pháp, thiết bị chuyên dụng có chức năng lọc gói tin giữa các phân đoạn mạng, lọc tầng ứng dụng, cảnh báo phát hiện và ngăn chặn xâm nhập trong hệ thống mạng của cơ quan, tổ chức	Chưa đáp ứng Mức 1.	Đã triển khai các giải pháp, thiết bị chuyên dụng có chức năng lọc gói tin giữa các phân đoạn mạng, lọc tầng ứng dụng, cảnh báo phát hiện và ngăn chặn xâm nhập trong hệ thống mạng của cơ quan, tổ chức.	Đáp ứng Mức 1 và có cơ chế đo lường, đánh giá tính hiệu quả của hoạt động triển khai các giải pháp, thiết bị chuyên dụng có chức năng lọc gói tin giữa các phân đoạn mạng, lọc tầng ứng dụng, cảnh báo phát hiện và ngăn chặn xâm nhập trong hệ thống mạng của cơ quan, tổ chức.	Đáp ứng Mức 2 và có cơ chế cải tiến liên tục dựa trên kết quả đánh giá để tối ưu hóa hoạt động triển khai các giải pháp, thiết bị chuyên dụng có chức năng lọc gói tin giữa các phân đoạn mạng, lọc tầng ứng dụng, cảnh báo phát hiện và ngăn chặn xâm nhập trong hệ thống mạng của cơ quan, tổ chức.	Giải pháp chuyên dụng có chức năng lọc gói tin giữa phân đoạn mạng
	II.13.4. Thiết lập cấu hình kiểm soát truy cập các cổng kết nối mạng	II.13.4.1. Thiết lập cấu hình trên các thiết bị mạng để kiểm soát truy cập các cổng kết nối mạng nếu thiết bị hỗ trợ.	Chưa đáp ứng Mức 1.	Đã thiết lập cấu hình trên các thiết bị mạng để kiểm soát truy cập các cổng kết nối mạng nếu thiết bị hỗ trợ.	Đáp ứng Mức 1 và có cơ chế đo lường, đánh giá tính hiệu quả của hoạt động thiết lập cấu hình kiểm soát truy cập các cổng kết nối mạng.	Đáp ứng Mức 2 và có cơ chế cải tiến liên tục dựa trên kết quả đánh giá để tối ưu hóa hoạt động thiết lập cấu hình kiểm soát truy cập các cổng kết nối mạng.	Báo cáo, tài liệu minh chứng.
		II.13.4.2. Thay đổi, tách biệt cổng quản trị ứng dụng với cổng cung cấp dịch vụ ứng dụng.	Chưa đáp ứng Mức 1.	Đã thay đổi, tách biệt cổng quản trị ứng dụng với cổng cung cấp dịch vụ ứng dụng.	Đáp ứng Mức 1 và có cơ chế đo lường, đánh giá tính hiệu quả của hoạt động thay đổi, tách biệt cổng quản trị ứng dụng với cổng cung cấp dịch vụ ứng dụng.	Đáp ứng Mức 2 và có cơ chế cải tiến liên tục dựa trên kết quả đánh giá để tối ưu hóa hoạt động thay đổi, tách biệt cổng quản trị ứng dụng với cổng cung cấp dịch vụ ứng dụng.	Báo cáo, tài liệu minh chứng.
	II.13.5. Thu thập thông tin dữ liệu mạng	II.13.5.1. Thu thập nhật ký luồng dữ liệu mạng và/ hoặc	Chưa đáp ứng Mức 1.	Đã thực hiện thu thập nhật ký luồng dữ liệu mạng và/ hoặc dữ liệu lưu lượng từ các thiết bị mạng	Đáp ứng Mức 1 và có cơ chế đo lường, đánh giá tính hiệu quả của hoạt động thu thập	Đáp ứng Mức 2 và có cơ chế cải tiến liên tục dựa trên kết quả đánh giá để tối ưu	Kiểm tra trên hệ thống luồng dữ liệu mạng và luồng dữ

		dữ liệu lưu lượng từ các thiết bị mạng để rà soát và đưa ra các cảnh báo		để rà soát và đưa ra các cảnh báo.	nhật ký luồng dữ liệu mạng và/ hoặc dữ liệu lưu lượng từ các thiết bị mạng để rà soát và đưa ra các cảnh báo.	hóa hoạt động thu thập nhật ký luồng dữ liệu mạng và/ hoặc dữ liệu lưu lượng từ các thiết bị mạng để rà soát và đưa ra các cảnh báo.	liệu từ các thiết bị mạng
	II.13.6. Điều chỉnh các ngưỡng cảnh báo sự kiện an ninh mạng	II.13.6.1. Điều chỉnh ngưỡng cảnh báo sự kiện an ninh mạng	Chưa đáp ứng Mức 1.	Đã thực hiện điều chỉnh ngưỡng cảnh báo sự kiện an ninh mạng, trong đó: - Cấp độ 4: tối thiểu 01 lần/06 tháng; - Cấp độ 5: tối thiểu 01 lần/01 tháng.	Đáp ứng Mức 1 và có cơ chế đo lường, đánh giá tính hiệu quả của hoạt động điều chỉnh ngưỡng cảnh báo sự kiện an ninh mạng.	Đáp ứng Mức 2 và có cơ chế cải tiến liên tục dựa trên kết quả đánh giá để tối ưu hóa hoạt động điều chỉnh ngưỡng cảnh báo sự kiện an ninh mạng.	Bản cập nhật ngưỡng cảnh báo sự kiện an ninh mạng
II.14. Nhân sự vận hành, quản trị hệ thống, bảo vệ an ninh mạng	II.14.1. Có bộ phận phụ trách về vận hành, quản trị hệ thống và bảo vệ an ninh mạng	II.14.1.1. Thành lập các bộ phận riêng biệt vận hành, quản trị hệ thống và bảo vệ an ninh mạng	Chưa đáp ứng Mức 1.	Đã thành lập các bộ phận riêng biệt vận hành, quản trị hệ thống và bảo vệ an ninh mạng; Nhân sự phụ trách về vận hành, quản trị hệ thống và bảo vệ an ninh mạng có trình độ chuyên môn về an ninh mạng, công nghệ thông tin; có cam kết bảo mật thông tin trong quá trình làm việc và sau khi nghỉ việc.	Đáp ứng Mức 1 và có cơ chế đo lường, đánh giá tính hiệu quả của hoạt động vận hành, quản trị hệ thống và bảo vệ an ninh mạng.	Đáp ứng Mức 2 và có cơ chế cải tiến liên tục dựa trên kết quả đánh giá để tối ưu hóa hoạt động vận hành, quản trị hệ thống và bảo vệ an ninh mạng.	Quy định thành lập các bộ phận riêng biệt vận hành, quản trị hệ thống và bảo vệ an ninh mạng.
		II.14.1.2. Có cơ chế hoạt động độc lập về chuyên môn giữa các bộ phận vận hành, quản trị hệ thống và bảo	Chưa đáp ứng Mức 1.	Đã thiết lập cơ chế hoạt động độc lập về chuyên môn giữa các bộ phận vận hành, quản trị hệ thống và bảo vệ an ninh mạng.	Đáp ứng Mức 1 và có cơ chế đo lường, đánh giá tính hiệu quả của cơ chế hoạt động độc lập về chuyên môn giữa các bộ phận vận hành, quản trị hệ thống và bảo vệ an ninh mạng.	- Đáp ứng Mức 2 và có cơ chế cải tiến liên tục dựa trên kết quả đánh giá để tối ưu hóa cơ chế hoạt động độc lập về chuyên môn giữa các bộ phận vận hành, quản	Quy định về cơ chế hoạt động độc lập chuyên môn

		vệ an ninh mạng				trị hệ thống và bảo vệ an ninh mạng.	
	II.14.2. Thiết lập và duy trì quy định sử dụng hệ thống thông tin, triển khai chương trình đào tạo tổng quan để nâng cao nhận thức an ninh mạng cho cán bộ, nhân viên	II.14.2.1. Thiết lập và duy trì một chương trình nâng cao nhận thức an ninh mạng cho toàn bộ cán bộ, nhân viên có sử dụng hệ thống thông tin	Chưa đáp ứng Mức 1.	Đã thiết lập và duy trì chương trình nâng cao nhận thức an ninh mạng cho toàn bộ cán bộ, nhân viên có sử dụng hệ thống thông tin.	Đáp ứng Mức 1 và có cơ chế đo lường, đánh giá tính hiệu quả của chương trình nâng cao nhận thức an ninh mạng.	Đáp ứng Mức 2 và có cơ chế cải tiến liên tục dựa trên kết quả đánh giá để tối ưu hóa nội dung và hình thức triển khai chương trình nâng cao nhận thức an ninh mạng.	Chương trình đào tạo nâng cao nhận thức và kỹ năng an ninh mạng
		II.14.2.2. Thu hồi quyền truy cập	Chưa đáp ứng Mức 1.	Đáp ứng tất cả các yêu cầu sau: - Khi cán bộ chấm dứt hoặc thay đổi công việc, tổ chức thực hiện thu hồi thẻ truy cập, thông tin được lưu trên các phương tiện lưu trữ, các trang thiết bị máy móc, phần cứng, phần mềm và các tài sản khác (nếu có) thuộc sở hữu của tổ chức. - Có quy trình và thực hiện vô hiệu hóa tất cả các quyền ra, vào, truy cập tài nguyên, quản trị hệ thống sau khi cán bộ thôi việc.	Đáp ứng Mức 1 và có cơ chế đo lường, đánh giá tính hiệu quả của hoạt động thu hồi quyền truy cập.	Đáp ứng Mức 2 và có cơ chế cải tiến liên tục dựa trên kết quả đánh giá để tối ưu hóa hoạt động thu hồi quyền truy cập.	Báo cáo, biên bản thu hồi quyền truy cập, tài liệu minh chứng.
		II.14.2.3. Cam kết giữ bí mật thông tin (áp dụng đối với hệ thống thông tin cấp độ 4 trở lên)	Chưa đáp ứng Mức 1.	Có cam kết giữ bí mật thông tin liên quan đến tổ chức sau khi nghỉ việc.	Đáp ứng Mức 1 và có cơ chế đo lường, đánh giá tính hiệu quả của cam kết giữ bí mật thông tin	Đáp ứng Mức 2 và có cơ chế cải tiến liên tục dựa trên kết quả đánh giá để tối ưu hóa cam kết giữ bí mật thông tin	Tài liệu minh chứng.

		II.14.2.4. Tiến hành đào tạo tối thiểu 01 lần/năm	Chưa đáp ứng Mức 1.	Đã tiến hành đào tạo theo chương trình nâng cao nhận thức an ninh mạng cho toàn bộ cán bộ, nhân viên có sử dụng hệ thống thông tin tối thiểu 01 lần/năm.	Đáp ứng Mức 1 và có cơ chế đo lường, đánh giá tính hiệu quả của hoạt động đào tạo.	Đáp ứng Mức 2 và có cơ chế cải tiến liên tục dựa trên kết quả đánh giá để tối ưu hóa hoạt động đào tạo.	Chứng chỉ hoặc kết quả đào tạo
	II.14.3. Thực hiện đào tạo kiến thức an ninh mạng theo từng vị trí, vai trò cụ thể (áp dụng đối với hệ thống thông tin cấp độ 4 trở lên)	II.14.3.1. Thực hiện đào tạo kiến thức chuyên môn và quy định pháp luật về an ninh mạng	Chưa đáp ứng Mức 1.	Đáp ứng tất cả các yêu cầu sau: - Đã thực hiện đào tạo kiến thức chuyên môn an ninh mạng theo từng vị trí, vai trò cụ thể; - Đào tạo nhận thức về quy định pháp luật liên quan, trách nhiệm pháp lý cho các cá nhân tham gia bảo vệ an ninh mạng.	Đáp ứng Mức 1 và có cơ chế đo lường, đánh giá tính hiệu quả của hoạt động đào tạo kiến thức chuyên môn và quy định pháp luật về an ninh mạng.	Đáp ứng Mức 2 và có cơ chế cải tiến liên tục dựa trên kết quả đánh giá để tối ưu hóa hoạt động đào tạo kiến thức chuyên môn và quy định pháp luật về an ninh mạng.	Kế hoạch đào tạo chuyên môn an ninh mạng
		II.14.3.2. Tiến hành đào tạo tối thiểu 01 lần/năm hoặc khi có thay đổi về các nhân sự liên quan trong tổ chức	Chưa đáp ứng Mức 3.			Đã tiến hành đào tạo kiến thức chuyên môn và quy định pháp luật về an ninh mạng tối thiểu 01 lần/năm hoặc khi có thay đổi về các nhân sự liên quan trong tổ chức.	Kết quả đào tạo tối thiểu 01 lần/năm
	II.14.4. Xây dựng khung năng lực cho nhân sự chuyên trách (áp dụng đối với hệ	II.14.4.1. Xây dựng khung năng lực tương ứng từng vị trí việc làm	Chưa đáp ứng Mức 1.	Đã xây dựng khung năng lực tương ứng từng vị trí việc làm, làm cơ sở cho việc tuyển dụng nhân sự chuyên trách vận hành, quản trị hệ thống, bảo vệ an ninh mạng.	Đáp ứng Mức 1 và có cơ chế đo lường, đánh giá tính hiệu quả của việc áp dụng khung năng lực.	Đáp ứng Mức 2 và có cơ chế cải tiến liên tục dựa trên kết quả đánh giá để tối ưu hóa khung năng lực.	Khung năng lực tương ứng với vị trí việc làm

	thống thông tin cấp độ 5)	II.14.4.2. Thực hiện đánh giá, kiểm tra trình độ chuyên môn đảm bảo phù hợp với vị trí làm việc	Chưa đáp ứng Mức 1.	Đã thực hiện đánh giá, kiểm tra trình độ chuyên môn đảm bảo phù hợp với vị trí làm việc.	Đáp ứng Mức 1 và có cơ chế đo lường, đánh giá tính hiệu quả của hoạt động đánh giá, kiểm tra trình độ chuyên môn.	Đáp ứng Mức 2 và có cơ chế cải tiến liên tục dựa trên kết quả đánh giá để tối ưu hóa hoạt động đánh giá, kiểm tra trình độ chuyên môn.	Kết quả đánh giá, kiểm tra trình độ chuyên môn đảm bảo với vị trí làm việc
II.15. Quản lý nhà cung cấp sản phẩm, dịch vụ	II.15.1. Thiết lập và duy trì bản kiểm kê các nhà cung cấp sản phẩm, dịch vụ	II.15.1.1. Thiết lập và duy trì bản kiểm kê các nhà cung cấp sản phẩm, dịch vụ	Chưa đáp ứng Mức 1.	Có phương án thiết lập và duy trì bản kiểm kê các nhà cung cấp sản phẩm, dịch vụ. Tối thiểu bao gồm: - Lập danh sách, theo dõi, cập nhật trạng thái các nhà cung cấp sản phẩm, dịch vụ; - Thực hiện phân loại các nhà cung cấp dịch vụ trong danh sách quản lý; - Đối với hệ thống thông tin cấp độ 5, các nhà cung cấp sản phẩm, dịch vụ an ninh mạng đủ điều kiện kinh doanh sản phẩm, dịch vụ an ninh mạng theo quy định của pháp luật; - Có văn bản xác định rõ phạm vi trách nhiệm của nhà cung cấp và tổ chức.	Đáp ứng Mức 1 và có cơ chế đo lường, đánh giá tính hiệu quả của hoạt động thiết lập và duy trì bản kiểm kê các nhà cung cấp sản phẩm, dịch vụ.	Đáp ứng Mức 2 và có cơ chế cải tiến liên tục dựa trên kết quả đánh giá để tối ưu hóa hoạt động thiết lập và duy trì bản kiểm kê các nhà cung cấp sản phẩm, dịch vụ.	Bản kiểm tra các nhà cung cấp dịch vụ, tài liệu minh chứng.
		II.15.1.2. Tần suất xem xét và cập nhật danh sách kiểm kê các nhà cung cấp sản phẩm, dịch vụ	Chưa đáp ứng Mức 3.			Đã xem xét và cập nhật danh sách tối thiểu 01 lần/năm hoặc khi xảy ra thay đổi ảnh hưởng đến danh sách này.	Báo cáo, tài liệu chứng minh.

	II.15.2. Thiết lập và duy trì quy định quản lý nhà cung cấp dịch vụ (áp dụng đối với hệ thống thông tin cấp độ 4 trở lên)	II.15.2.1. Xây dựng, ban hành và đảm bảo tuân thủ quy định quản lý các nhà cung cấp dịch vụ.	Chưa đáp ứng Mức 1.	Đã xây dựng và ban hành quy định quản lý các nhà cung cấp dịch vụ.	Đáp ứng Mức 1 và có cơ chế đo lường, đánh giá tính hiệu quả của việc thực hiện quy định quản lý các nhà cung cấp dịch vụ.	Đáp ứng Mức 2 và có cơ chế cải tiến liên tục dựa trên kết quả đánh giá để tối ưu hóa quy định quản lý các nhà cung cấp dịch vụ.	Chính sách quản lý nhà cung cấp dịch vụ
		II.15.2.2. Đánh giá và cập nhật quy định quản lý nhà cung cấp dịch vụ	Chưa đáp ứng Mức 3.			Đã thực hiện đánh giá và cập nhật quy định tối thiểu 01 lần/năm hoặc khi xảy ra thay đổi ảnh hưởng đến quy định này.	Bản cập nhật chính sách quản lý các nhà cung cấp dịch vụ
	II.15.3. Đảm bảo các hợp đồng cung cấp dịch vụ có kèm theo các yêu cầu bảo mật (áp dụng đối với hệ thống thông tin cấp độ 4 trở lên)	II.15.3.1. Đảm bảo các hợp đồng với nhà cung cấp dịch vụ an ninh mạng bao gồm đầy đủ yêu cầu về bảo mật	Chưa đáp ứng Mức 1.	Các hợp đồng với nhà cung cấp dịch vụ an ninh mạng bao gồm đầy đủ yêu cầu về bảo mật.	Đáp ứng Mức 1 và có cơ chế đo lường, đánh giá tính hiệu quả của việc đưa yêu cầu bảo mật vào hợp đồng nhà cung cấp.	Đáp ứng Mức 2 và có cơ chế cải tiến liên tục dựa trên kết quả đánh giá để tối ưu hóa yêu cầu bảo mật trong hợp đồng nhà cung cấp.	Báo cáo xác minh các hợp đồng của nhà cung cấp dịch vụ
		II.15.3.2. Đánh giá và cập nhật hợp đồng của nhà cung cấp dịch vụ khi gia hạn để đảm bảo đầy đủ các yêu cầu bảo mật.	Chưa đáp ứng Mức 1.	Đã thực hiện đánh giá và cập nhật hợp đồng của nhà cung cấp dịch vụ khi gia hạn để đảm bảo đầy đủ các yêu cầu bảo mật.	Đáp ứng Mức 1 và có cơ chế đo lường, đánh giá tính hiệu quả của hoạt động đánh giá và cập nhật yêu cầu bảo mật khi gia hạn hợp đồng	Đáp ứng Mức 2 và có cơ chế cải tiến liên tục dựa trên kết quả đánh giá để tối ưu hóa hoạt động đánh giá và cập nhật yêu cầu bảo mật khi gia hạn hợp đồng	Bản đánh giá và cập nhật hợp đồng của các nhà cung cấp dịch vụ
	II.15.4. Thực hiện theo dõi các nhà cung cấp dịch vụ (áp dụng đối với hệ	II.15.4.1. Giám sát các nhà cung cấp dịch vụ thực hiện quy định quản	Chưa đáp ứng Mức 1.	Đã thực hiện giám sát các nhà cung cấp dịch vụ thực hiện quy định quản lý cung cấp dịch vụ của tổ chức.	Đáp ứng Mức 1 và có cơ chế đo lường, đánh giá tính hiệu quả của hoạt động giám sát nhà cung cấp dịch vụ.	Đáp ứng Mức 2 và có cơ chế cải tiến liên tục dựa trên kết quả đánh giá để tối ưu hóa hoạt động giám	Nhật ký giám sát sự tuân thủ của các nhà cung cấp dịch vụ

	thống thông tin cấp độ 4 trở lên)	lý cung cấp dịch vụ của tổ chức				sát nhà cung cấp dịch vụ.	
	II.15.5. Rà soát vấn đề bảo mật khi kết thúc hợp đồng với các nhà cung cấp dịch vụ (áp dụng đối với hệ thống thông tin cấp độ 4 trở lên)	II.15.5.1. Rà soát vấn đề bảo mật khi kết thúc hợp đồng với các nhà cung cấp dịch vụ	Chưa đáp ứng Mức 1.	Đã thực hiện rà soát vấn đề bảo mật khi kết thúc hợp đồng; thu hồi quyền truy cập, xử lý dữ liệu và lập biên bản thu hồi.	Đáp ứng Mức 1 và có cơ chế đo lường, đánh giá tính hiệu quả của hoạt động rà soát vấn đề bảo mật khi kết thúc hợp đồng với các nhà cung cấp dịch vụ.	Đáp ứng Mức 2 và có cơ chế cải tiến liên tục dựa trên kết quả đánh giá để tối ưu hóa hoạt động rà soát vấn đề bảo mật khi kết thúc hợp đồng với các nhà cung cấp dịch vụ.	Báo cáo thực hiện rà soát bảo mật khi kết thúc hợp đồng với các nhà cung cấp dịch vụ
II.16. Phát triển ứng dụng an toàn	II.16.1. Thiết lập và duy trì quy trình phát triển ứng dụng an toàn	II.16.1.1. Xây dựng, ban hành và đảm bảo tuân thủ quy trình phát triển ứng dụng an toàn	Chưa đáp ứng Mức 1.	Đã xây dựng, ban hành và đảm bảo tuân thủ quy trình phát triển ứng dụng an toàn.	Đáp ứng Mức 1 và có cơ chế đo lường, đánh giá tính hiệu quả của quy trình phát triển ứng dụng an toàn.	Đáp ứng Mức 2 và có cơ chế cải tiến liên tục dựa trên kết quả đánh giá để tối ưu hóa quy trình phát triển ứng dụng an toàn	Quy trình phát triển ứng dụng an toàn
		II.16.1.2. Đánh giá và cập nhật quy trình phát triển ứng dụng an toàn	Chưa đáp ứng Mức 3.			Đã thực hiện đánh giá và cập nhật quy trình tối thiểu 01 lần/năm hoặc khi xảy ra các thay đổi có thể ảnh hưởng đến quy trình.	Bản cập nhật quy trình phát triển ứng dụng an toàn
		II.16.1.3. Yêu cầu đối với các phần mềm phát triển thuê khoán	Chưa đáp ứng Mức 1.	- Đối với các phần mềm phát triển thuê khoán, yêu cầu: + Có biên bản, hợp đồng và cam kết bảo mật đối với bên thuê khoán các nội dung liên quan đến phát	Đáp ứng Mức 1 và có cơ chế đo lường, đánh giá tính hiệu quả của hoạt động phát triển phần mềm thuê khoán.	Đáp ứng Mức 2 và có cơ chế cải tiến liên tục dựa trên kết quả đánh giá để tối ưu hóa hoạt động phát triển phần mềm thuê khoán.	Biên bản, hợp đồng và cam kết bảo mật đối với các bên thuê khoán

				triển phần mềm thuê khoán; + Yêu cầu nhà phát triển cung cấp mã nguồn phần mềm. Trong trường hợp không thể cung cấp mã nguồn phần mềm, chủ quản hệ thống yêu cầu các bên thuê khoán cung cấp chứng chỉ đánh giá an toàn độc lập hoặc thực hiện các biện pháp kiểm thử xâm nhập, giám sát rủi ro thay thế và ký cam kết chịu trách nhiệm pháp lý về tính an toàn của phần mềm. - Đối với hệ thống thông tin cấp độ 4 trở lên: + Kiểm thử phần mềm trên môi trường thử nghiệm trước khi đưa vào sử dụng. + Kiểm tra, đánh giá an ninh mạng của phần mềm trước khi đưa vào sử dụng. + Khi thay đổi mã nguồn, kiến trúc phần mềm thực hiện kiểm tra, đánh giá an ninh mạng cho phần mềm. + Có cam kết của bên phát triển về bảo đảm tính bí mật và bản quyền của phần mềm phát triển.			
	II.16.2. Thiết lập và duy trì quy trình tiếp	II.16.2.1. Xây dựng, ban hành và đảm bảo	Chưa đáp ứng Mức 1.	Đã ban hành quy trình tiếp nhận và xử lý báo cáo lỗ hổng bảo mật phần mềm,	Đáp ứng Mức 1 và có cơ chế đo lường, đánh giá tính hiệu quả của	Đáp ứng Mức 2 và có cơ chế cải tiến liên tục dựa trên kết quả	Quy trình tiếp nhận và xử lý báo

	nhận và xử lý lỗ hổng bảo mật phần mềm	tuân thủ quy trình tiếp nhận và xử lý báo cáo về lỗ hổng bảo mật phần mềm		bao gồm cả việc cung cấp phương tiện để các cá nhân, tổ chức bên ngoài báo cáo.	quy trình tiếp nhận và xử lý báo cáo lỗ hổng bảo mật phần mềm.	đánh giá để tối ưu hóa quy trình tiếp nhận và xử lý báo cáo lỗ hổng bảo mật phần mềm.	cáo về lỗ hổng bảo mật
		II.16.2.2. Quản lý, theo dõi lỗ hổng bảo mật phần mềm (áp dụng đối với hệ thống thông tin cấp độ 5)	Chưa đáp ứng Mức 1.	Đã quản lý và theo dõi lỗ hổng bảo mật phần mềm, bao gồm xếp hạng mức độ nghiêm trọng và chỉ số đo lường thời gian để xác định, phân tích và khắc phục các lỗ hổng.	Đáp ứng Mức 1 và có cơ chế đo lường, đánh giá tính hiệu quả của hoạt động quản lý và theo dõi lỗ hổng bảo mật phần mềm.	Đáp ứng Mức 2 và có cơ chế cải tiến liên tục dựa trên kết quả đánh giá để tối ưu hóa hoạt động quản lý và theo dõi lỗ hổng bảo mật phần mềm.	Hệ thống đánh giá mức độ nghiêm trọng và quy trình xử lý các lỗ hổng bảo mật theo mức độ nghiêm trọng
		II.16.2.3. Đánh giá và cập nhật quy trình tiếp nhận và xử lý lỗ hổng bảo mật phần mềm	Chưa đáp ứng Mức 3.			Đã đánh giá và cập nhật quy trình tối thiểu 01 lần/năm hoặc khi xảy ra các thay đổi có thể ảnh hưởng đến quy trình.	Bản cập nhật quy trình phát triển ứng dụng an toàn
	II.16.3. Thực hiện phân tích nguyên nhân cốt lõi của lỗ hổng bảo mật (áp dụng đối với hệ thống thông tin cấp độ 4 trở lên)	II.16.3.1. Thực hiện phân tích nguyên nhân cốt lõi của các lỗ hổng bảo mật	Chưa đáp ứng Mức 1.	Đã thực hiện phân tích nguyên nhân cốt lõi của các lỗ hổng bảo mật.	Đáp ứng Mức 1 và có cơ chế đo lường, đánh giá tính hiệu quả của hoạt động phân tích nguyên nhân cốt lõi của các lỗ hổng bảo mật.	Đáp ứng Mức 2 và có cơ chế cải tiến liên tục dựa trên kết quả đánh giá để tối ưu hóa hoạt động phân tích nguyên nhân cốt lõi của các lỗ hổng bảo mật.	Báo cáo phân tích nguyên nhân cốt lõi các lỗ hổng bảo mật
	II.16.4. Thiết lập và quản trị hệ thống kiểm kê các cấu thành phần mềm của bên	II.16.4.1. Thiết lập và quản lý một danh sách cập nhật các thành phần của bên thứ ba	Chưa đáp ứng Mức 1.	Đã thiết lập và cập nhật danh sách các thành phần bên thứ ba được sử dụng trong quá trình phát triển (thư viện, mô đun…) và các thành phần dự kiến sẽ	Đáp ứng Mức 1 và có cơ chế đo lường, đánh giá tính hiệu quả của hoạt động thiết lập và cập nhật danh sách các thành phần bên thứ ba.	Đáp ứng Mức 2 và có cơ chế cải tiến liên tục dựa trên kết quả đánh giá để tối ưu hóa hoạt động thiết lập và cập nhật danh	Danh sách cập nhật các thành phần của bên thứ ba

	thứ ba (áp dụng đối với hệ thống thông tin cấp độ 4 trở lên)			sử dụng trong tương lai để phát triển phần mềm.		sách các thành phần bên thứ ba.	
		II.16.4.2. Danh sách bao gồm các rủi ro an ninh mạng mà mỗi thành phần bên thứ ba có thể gây ra	Chưa đáp ứng Mức 1.	Đã đánh giá và xác định rủi ro an ninh mạng của các thành phần bên thứ ba có thể gây ra.	Đáp ứng Mức 1 và có cơ chế đo lường, đánh giá tính hiệu quả của hoạt động đánh giá và xác định rủi ro an ninh mạng của các thành phần bên thứ ba có thể gây ra.	Đáp ứng Mức 2 và có cơ chế cải tiến liên tục dựa trên kết quả đánh giá để tối ưu hóa hoạt động đánh giá và xác định rủi ro an ninh mạng của các thành phần bên thứ ba có thể gây ra.	Danh sách bao gồm các rủi ro an ninh mạng mà mỗi bên thứ 3 có thể gây ra
		II.16.4.3. Đánh giá và cập nhật danh sách	Chưa đáp ứng Mức 3.			Đã thực hiện đánh giá và cập nhật danh sách, trong đó: - Cấp độ 4: tối thiểu 01 lần/01 quý; - Cấp độ 5: tối thiểu 01 lần/01 tháng.	Bản cập nhật danh sách các rủi ro
	II.16.5. Tách biệt môi trường cho các hoạt động phát triển, kiểm thử và vận hành (áp dụng đối với hệ thống thông tin cấp độ 4 trở lên)	II.16.5.1. Duy trì việc tách biệt môi trường vận hành chính thức, môi trường kiểm thử và môi trường phát triển	Chưa đáp ứng Mức 1.	Đã duy trì việc tách biệt môi trường vận hành chính thức, môi trường kiểm thử và môi trường phát triển; trong đó yêu cầu không lưu trữ thông tin xác thực, thông tin bí mật trên mã nguồn ứng dụng.	Đáp ứng Mức 1 và có cơ chế đo lường, đánh giá tính hiệu quả của việc duy trì việc tách biệt môi trường và bảo vệ thông tin bí mật.	Đáp ứng Mức 2 và có cơ chế cải tiến liên tục dựa trên kết quả đánh giá để tối ưu hóa việc duy trì tách biệt môi trường và bảo vệ thông tin bí mật.	Biện pháp tách biệt môi trường sản xuất và môi trường phát triển sản phẩm
	II.16.6. Đào tạo về bảo mật và lập trình an toàn (áp dụng đối với hệ thống thông tin	II.16.6.1. Tổ chức đào tạo về bảo mật và lập trình an toàn	Chưa đáp ứng Mức 1.	Đảm bảo tất cả nhân viên phát triển phần mềm được đào tạo về trách nhiệm và phương thức phát triển phần mềm an toàn đối với từng môi trường/giải pháp cụ thể.	Đáp ứng Mức 1 và có cơ chế đo lường, đánh giá tính hiệu quả của hoạt động đào tạo về bảo mật và lập trình an toàn.	Đáp ứng Mức 2 và có cơ chế cải tiến liên tục dựa trên kết quả đánh giá để tối ưu hóa hoạt động đào tạo về bảo mật và lập trình an toàn.	Kế hoạch đào tạo cho nhân viên về cách lập trình an toàn cho môi trường phát triển cụ thể và trách nhiệm của họ

	cấp độ 4 trở lên)	II.16.6.2. Thực hiện đào tạo tối thiểu 01 lần/năm	Chưa đáp ứng Mức 3.			Đã thực hiện đào tạo về bảo mật và lập trình an toàn tối thiểu 01 lần/năm.	Chứng chỉ hoặc kết quả đánh giá đào tạo
	II.16.7. Kết hợp các nguyên tắc bảo mật trong kiến trúc ứng dụng	II.16.7.1. Kết hợp các nguyên tắc bảo mật trong quá trình xây dựng kiến trúc ứng dụng	Chưa đáp ứng Mức 1.	Đã kết hợp các nguyên tắc bảo mật trong quá trình xây dựng kiến trúc ứng dụng. Trong đó bao gồm nhưng không giới hạn các yêu cầu: - Có chức năng kiểm tra tính hợp lệ của thông tin, dữ liệu đầu vào trước khi xử lý; - Có chức năng kiểm tra tính hợp lệ của thông tin, dữ liệu đầu ra trước khi gửi về máy yêu cầu; - Có phương án bảo vệ ứng dụng chống lại những dạng tấn công phổ biến; - Có chức năng kiểm soát lỗi, thông báo lỗi từ ứng dụng; - Không lưu trữ thông tin xác thực, thông tin bí mật trên mã nguồn ứng dụng. - Đối với hệ thống thông tin cấp độ 4 trở lên, có chức năng tạo lập, duy trì và quản lý phiên làm việc an toàn.	Đáp ứng Mức 1 và có cơ chế đo lường, đánh giá tính hiệu quả của việc kết hợp các nguyên tắc bảo mật trong quá trình xây dựng kiến trúc ứng dụng.	Đáp ứng Mức 2 và có cơ chế cải tiến liên tục dựa trên kết quả đánh giá để tối ưu hóa việc kết hợp các nguyên tắc bảo mật trong quá trình xây dựng kiến trúc ứng dụng.	Nguyên tắc thiết kế an toàn trong xây dựng kiến trúc ứng dụng
	II.16.8. Tận dụng các mô-đun hoặc dịch vụ đã được	II.16.8.1. Tận dụng mô-đun hoặc dịch vụ đã được kiểm	Chưa đáp ứng Mức 1.	Đã tận dụng mô-đun hoặc dịch vụ đã được kiểm chứng cho các thành phần bảo mật của ứng dụng.	Đáp ứng Mức 1 và có cơ chế đo lường, đánh giá tính hiệu quả của việc tận dụng mô-đun	Đáp ứng Mức 2 và có cơ chế cải tiến liên tục dựa trên kết quả đánh giá để tối ưu	Danh sách các mô-đun và các dịch vụ đã được kiểm chứng

	kiểm chứng cho các thành phần bảo mật ứng dụng (áp dụng đối với hệ thống thông tin cấp độ 4 trở lên)	chứng cho các thành phần bảo mật của ứng dụng			hoặc dịch vụ đã được kiểm chứng cho các thành phần bảo mật của ứng dụng.	hóa việc tận dụng mô-đun hoặc dịch vụ đã được kiểm chứng cho các thành phần bảo mật của ứng dụng.	
		II.16.8.2. Chỉ sử dụng thuật toán mã hoá mạnh, được chuẩn hoá và đánh giá rộng rãi	Chưa đáp ứng Mức 1.	Chỉ sử dụng thuật toán mã hóa mạnh (chưa được các tổ chức quốc tế công bố điểm yếu), được chuẩn hóa và đánh giá rộng rãi theo yêu cầu.	Đáp ứng Mức 1 và có cơ chế đo lường, đánh giá tính hiệu quả của việc sử dụng thuật toán mã hóa.	Đáp ứng Mức 2 và có cơ chế cải tiến liên tục dựa trên kết quả đánh giá để tối ưu hóa việc sử dụng thuật toán mã hóa.	Danh sách các thuật toán mã hoá có thể được sử dụng
		II.16.8.3. Ghi nhật ký kiểm toán hành vi của người dùng trong sản phẩm	Chưa đáp ứng Mức 1.	Đã ghi nhật ký kiểm toán hành vi của người dùng trong sản phẩm.	Đáp ứng Mức 1 và có cơ chế đo lường, đánh giá tính hiệu quả của hoạt động ghi nhật ký kiểm toán hành vi của người dùng trong sản phẩm.	Đáp ứng Mức 2 và có cơ chế cải tiến liên tục dựa trên kết quả đánh giá để tối ưu hóa hoạt động ghi nhật ký kiểm toán hành vi của người dùng trong sản phẩm.	Nhật ký kiểm toán các hành vi của người dùng trong sản phẩm
	II.16.9. Tiến hành kiểm tra an ninh, an toàn các ứng dụng	II.16.9.1. Kiểm tra lỗ hổng bảo mật trong mã nguồn, thư viện và thành phần mở rộng.	Chưa đáp ứng Mức 1.	Đã thực hiện kiểm tra các lỗ hổng bảo mật trong mã nguồn được phát triển, lỗ hổng trong các thư viện, thành phần mở rộng của bên thứ ba mà ứng dụng sử dụng.	Đáp ứng Mức 1 và có cơ chế đo lường, đánh giá tính hiệu quả của hoạt động kiểm tra lỗ hổng bảo mật trong mã nguồn, thư viện và thành phần mở rộng.	Đáp ứng Mức 2 và có cơ chế cải tiến liên tục dựa trên kết quả đánh giá để tối ưu hóa hoạt động kiểm tra lỗ hổng bảo mật trong mã nguồn, thư viện và thành phần mở rộng.	Báo cáo kiểm tra lỗ hổng bảo mật
		II.16.9.2. Kiểm thử xâm nhập và khắc phục các lỗ hổng bảo mật trước khi	Chưa đáp ứng Mức 1.	Đã thực hiện kiểm thử xâm nhập và khắc phục các lỗ hổng bảo mật trước khi đưa vào vận hành chính thức.	Đáp ứng Mức 1 và có cơ chế đo lường, đánh giá tính hiệu quả của hoạt động kiểm thử xâm nhập và khắc	Đáp ứng Mức 2 và có cơ chế cải tiến liên tục dựa trên kết quả đánh giá để tối ưu hóa hoạt động kiểm	Báo cáo kiểm thử xâm nhập

		đưa vào vận hành chính thức (áp dụng đối với hệ thống thông tin cấp độ 4 trở lên).			phục các lỗ hổng bảo mật trước khi đưa vào vận hành chính thức.	thử xâm nhập và khắc phục các lỗ hổng bảo mật trước khi đưa vào vận hành chính thức.	
II.17. Quản trị ứng phó sự cố an ninh mạng	II.17.1. Thành lập lực lượng ứng phó sự cố an ninh mạng	II.17.1.1. Chỉ định một người chủ chốt và ít nhất một người dự phòng để quản lý quy trình ứng phó sự cố an ninh mạng	Chưa đáp ứng Mức 1.	Đã chỉ định một người chủ chốt và ít nhất một người dự phòng để quản lý quy trình ứng phó sự cố an ninh mạng.	Đáp ứng Mức 1 và có cơ chế đo lường, đánh giá tính hiệu quả của việc chỉ định một người chủ chốt và ít nhất một người dự phòng để quản lý quy trình ứng phó sự cố an ninh mạng.	Đáp ứng Mức 2 và có cơ chế cải tiến liên tục dựa trên kết quả đánh giá để tối ưu hóa việc chỉ định và vận hành vai trò chủ chốt/dự phòng	Danh sách người chủ chốt và những người dự phòng để quản lý quy trình ứng phó sự cố an ninh mạng
		II.17.1.2. Thiết lập và duy trì đầu mối liên hệ, phối hợp với các cơ quan, tổ chức có thẩm quyền	Chưa đáp ứng Mức 1.	Đã thiết lập và duy trì đầu mối liên hệ, phối hợp với các cơ quan, tổ chức có thẩm quyền quản lý nhà nước về an ninh mạng, cơ quan điều hành Liên minh ứng phó, khắc phục sự cố an ninh mạng quốc gia	Đáp ứng Mức 1 và có cơ chế đo lường, đánh giá tính hiệu quả của việc thiết lập và duy trì đầu mối liên hệ, phối hợp với các cơ quan, tổ chức có thẩm quyền.	Đáp ứng Mức 2 và có cơ chế cải tiến liên tục dựa trên kết quả đánh giá để tối ưu hóa việc thiết lập và duy trì đầu mối liên hệ, phối hợp với các cơ quan, tổ chức có thẩm quyền.	Thông tin liên hệ, tài liệu minh chứng.
		II.17.1.3. Thiết lập và duy trì đầu mối liên lạc để báo cáo sự cố	Chưa đáp ứng Mức 1.	Đã thiết lập và duy trì đầu mối liên lạc để báo cáo sự cố; xác minh thông tin liên hệ của các cơ quan, tổ chức hỗ trợ điều phối ứng phó sự cố hàng năm để đảm bảo thông tin được cập nhật.	Đáp ứng Mức 1 và có cơ chế đo lường, đánh giá tính hiệu quả của hoạt động thiết lập và duy trì đầu mối liên lạc để báo cáo sự cố.	Đáp ứng Mức 2 và có cơ chế cải tiến liên tục dựa trên kết quả đánh giá để tối ưu hóa hoạt động thiết lập và duy trì đầu mối liên lạc để báo cáo sự cố.	Bản cập nhật thông tin liên hệ hàng năm
		II.17.1.4. Phân công vị trí, vai	Chưa đáp ứng Mức 1.	Đã phân công vị trí, vai trò và trách nhiệm chính của	Đáp ứng Mức 1 và có cơ chế đo lường, đánh	Đáp ứng Mức 2 và có cơ chế cải tiến liên	Danh sách phân công vị trí, vai trò

		trò và trách nhiệm chính của từng thành viên trong lực lượng tham gia ứng phó sự cố		từng thành viên trong lực lượng tham gia ứng phó sự cố.	giá tính hiệu quả của việc phân công vị trí, vai trò và trách nhiệm chính của từng thành viên trong lực lượng tham gia ứng phó sự cố.	tục dựa trên kết quả đánh giá để tối ưu hóa việc phân công vị trí, vai trò và trách nhiệm chính của từng thành viên trong lực lượng tham gia ứng phó sự cố.	và trách nhiệm từng thành viên
		II.17.1.5. Quy định về trách nhiệm phối hợp với lực lượng ứng phó sự cố an ninh mạng của các phòng ban có liên quan	Chưa đáp ứng Mức 1.	Đã ban hành quy định về trách nhiệm phối hợp với lực lượng ứng phó sự cố an ninh mạng của các phòng ban có liên quan.	Đáp ứng Mức 1 và có cơ chế đo lường, đánh giá tính hiệu quả của việc thực hiện quy định về trách nhiệm phối hợp với lực lượng ứng phó sự cố an ninh mạng của các phòng ban có liên quan.	Đáp ứng Mức 2 và có cơ chế cải tiến liên tục dựa trên kết quả đánh giá để tối ưu hóa hoạt động phối hợp với lực lượng ứng phó sự cố an ninh mạng của các phòng ban có liên quan.	Quy định về trách nhiệm phối hợp với các lực lượng
	II.17.2. Thiết lập và duy trì quy trình nội bộ để báo cáo sự cố an ninh mạng	II.17.2.1. Thiết lập và duy trì quy trình nội bộ để báo cáo sự cố an ninh mạng	Chưa đáp ứng Mức 1.	Đã thiết lập và duy trì quy trình nội bộ để báo cáo sự cố an ninh mạng.	Đáp ứng Mức 1 và có cơ chế đo lường, đánh giá tính hiệu quả của quy trình nội bộ để báo cáo sự cố an ninh mạng.	Đáp ứng Mức 2 và có cơ chế cải tiến liên tục dựa trên kết quả đánh giá để tối ưu hóa quy trình nội bộ để báo cáo sự cố an ninh mạng.	Quy trình nội bộ để báo cáo sự cố an ninh mạng
		II.17.2.2. Thực hiện phân nhóm sự cố an ninh mạng	Chưa đáp ứng Mức 1.	Đã thực hiện phân nhóm sự cố an ninh mạng.	Đáp ứng Mức 1 và có cơ chế đo lường, đánh giá tính hiệu quả của việc phân nhóm sự cố an ninh mạng.	Đáp ứng Mức 2 và có cơ chế cải tiến liên tục dựa trên kết quả đánh giá để tối ưu hóa việc phân nhóm sự cố an ninh mạng.	Danh sách phân nhóm sự cố an ninh mạng
		II.17.2.3. Đánh giá và cập nhật quy trình	Chưa đáp ứng Mức 3.			Đã thực hiện đánh giá và cập nhật quy trình tối thiểu 01 lần/năm hoặc khi xảy	Kết quả cập nhật quy trình định kỳ

						ra các thay đổi ảnh hưởng đến quy trình.	
	II.17.3. Thiết lập và duy trì quy trình ứng phó sự cố an ninh mạng	II.17.3.1. Thiết lập và duy trì một quy trình ứng phó sự cố	Chưa đáp ứng Mức 1.	Đã thiết lập và duy trì một quy trình ứng phó sự cố, đảm bảo có cơ chế phối hợp với các cơ quan chức năng, các nhóm chuyên gia, bên cung cấp dịch vụ khắc phục sự cố an ninh mạng.	Đáp ứng Mức 1 và có cơ chế đo lường, đánh giá tính hiệu quả của quy trình ứng phó sự cố.	Đáp ứng Mức 2 và có cơ chế cải tiến liên tục dựa trên kết quả đánh giá để tối ưu hóa quy trình ứng phó sự cố.	Quy trình ứng phó sự cố
		II.17.3.2. Đánh giá và cập nhật quy trình	Chưa đáp ứng Mức 3.			Đã thực hiện đánh giá và cập nhật quy trình tối thiểu 01 lần/năm hoặc khi xảy ra các thay đổi ảnh hưởng đến quy trình.	Kết quả cập nhật quy trình định kỳ
	II.17.4. Thiết lập cơ chế (kênh kỹ thuật) liên lạc trong quá trình xử lý sự cố (áp dụng đối với hệ thống thông tin cấp độ 4 trở lên)	II.17.4.1. Thiết lập cơ chế chính và cơ chế phụ sử dụng để giao tiếp và báo cáo trong xử lý sự cố an ninh mạng	Chưa đáp ứng Mức 1.	Đã thiết lập cơ chế chính và cơ chế phụ sử dụng để giao tiếp và báo cáo trong xử lý sự cố an ninh mạng.	Đáp ứng Mức 1 và có cơ chế đo lường, đánh giá tính hiệu quả của cơ chế liên lạc trong quá trình xử lý sự cố.	Đáp ứng Mức 2 và có cơ chế cải tiến liên tục dựa trên kết quả đánh giá để tối ưu hóa cơ chế liên lạc trong quá trình xử lý sự cố.	Cơ chế chính và cơ chế phụ để giao tiếp và báo cáo
		II.17.4.2. Đánh giá và cập nhật cơ chế liên lạc	Chưa đáp ứng Mức 3.			Đã thực hiện đánh giá và cập nhật cơ chế liên lạc tối thiểu 01 lần/năm hoặc khi xảy ra các thay đổi ảnh hưởng đến cơ chế.	Bản cập nhật cơ chế liên lạc
	II.17.5. Thực hiện đánh giá sau sự cố an ninh mạng (áp	II.17.5.1. Thực hiện đánh giá sau sự cố an ninh mạng	Chưa đáp ứng Mức 1.	Đã thực hiện đánh giá sau sự cố an ninh mạng.	Đáp ứng Mức 1 và có cơ chế đo lường, đánh giá tính hiệu quả của hoạt động đánh giá sau sự cố an ninh mạng.	Đáp ứng Mức 2 và có cơ chế cải tiến liên tục dựa trên kết quả đánh giá để tối ưu hóa hoạt động đánh	Bản đánh giá sau sự cố và các biện pháp ngăn sự cố tái diễn

	dụng đối với hệ thống thông tin cấp độ 4 trở lên)					giá sau sự cố an ninh mạng.	
	II.17.6. Định kỳ diễn tập ứng phó sự cố an ninh mạng (áp dụng đối với hệ thống thông tin cấp độ 4 trở lên)	II.17.6.1. Lập kế hoạch và thực hiện diễn tập các kịch bản ứng phó sự cố	Chưa đáp ứng Mức 1.	Đã lập kế hoạch và thực hiện diễn tập các kịch bản ứng phó sự cố định kỳ tối thiểu 01 lần/năm.	Đáp ứng Mức 1 và có cơ chế đo lường, đánh giá tính hiệu quả của hoạt động lập kế hoạch và thực hiện diễn tập các kịch bản ứng phó sự cố.	Đáp ứng Mức 2 và có cơ chế cải tiến liên tục dựa trên kết quả đánh giá để tối ưu hóa hoạt động lập kế hoạch và thực hiện diễn tập các kịch bản ứng phó sự cố.	Kế hoạch diễn tập các kịch bản ứng cứu sự cố
	II.17.7. Triển khai và duy trì các ngưỡng sự cố an ninh mạng (áp dụng đối với hệ thống thông tin cấp độ 4 trở lên)	II.17.7.1. Thiết lập và duy trì các ngưỡng sự cố an ninh mạng	Chưa đáp ứng Mức 1.	Đã thiết lập và duy trì các ngưỡng sự cố an ninh mạng.	Đáp ứng Mức 1 và có cơ chế đo lường, đánh giá tính hiệu quả của hoạt động thiết lập và duy trì các ngưỡng sự cố an ninh mạng.	Đáp ứng Mức 2 và có cơ chế cải tiến liên tục dựa trên kết quả đánh giá để tối ưu hóa hoạt động thiết lập và duy trì các ngưỡng sự cố an ninh mạng.	Bảng phân loại các ngưỡng sự cố an ninh mạng
		II.17.7.2. Đánh giá và cập nhật ngưỡng sự cố an ninh mạng	Chưa đáp ứng Mức 3.			Đã thực hiện đánh giá và cập nhật ngưỡng định kỳ hoặc khi xảy ra các thay đổi ảnh hưởng đến ngưỡng, trong đó: - Cấp độ 4: tối thiểu 01 lần/01 năm; - Cấp độ 5: tối thiểu 01 lần/06 tháng.	Bản cập nhật phân loại các ngưỡng sự cố an ninh mạng
II.18. Quản lý kiểm tra an ninh mạng	II.18.1. Thiết lập và duy trì một chương trình kiểm thử xâm nhập	II.18.1.1. Thiết lập và duy trì một chương trình kiểm thử xâm nhập	Chưa đáp ứng Mức 1.	Đã thiết lập chương trình kiểm thử xâm nhập phù hợp với quy mô, mức độ phức tạp và trạng thái của	Đáp ứng Mức 1 và có cơ chế đo lường, đánh giá tính hiệu quả của chương trình kiểm thử xâm nhập.	Đáp ứng Mức 2 và có cơ chế cải tiến liên tục dựa trên kết quả đánh giá để tối ưu	Kịch bản chương trình kiểm thử xâm nhập phù hợp với quy mô, mức độ phức tạp và

				tổ chức và đáp ứng một số nội dung sau: - Về yêu cầu: hoạt động kiểm thử xâm nhập được phê duyệt về phạm vi, thời gian, phương pháp, đầu mối phối hợp, phương án đảm bảo an ninh mạng và phương án xử lý dữ liệu thu được; đối với hệ thống đang vận hành, thời điểm và cách thức kiểm thử được lựa chọn phù hợp để không làm gián đoạn dịch vụ, ưu tiên thực hiện trên môi trường phát triển hoặc trong thời gian đã được phê duyệt. - Về phạm vi tiến hành: kiểm tra một phần hoặc toàn bộ hạ tầng công nghệ thông tin của tổ chức; - Về tần suất: hàng quý, nửa năm, một năm hoặc đột xuất; - Về các giới hạn: xác định các hành vi tấn công bị cấm (tấn công vật lý, tấn công lừa đảo, tấn công phi kỹ thuật…); - Về cách phản ứng của tổ chức: có thực hiện việc ngăn chặn hay không, cơ chế kiểm soát thông tin (về cuộc kiểm thử) trong nội bộ.		hóa chương trình kiểm thử xâm nhập.	trạng thái của tổ chức

	II.18.2. Định kỳ thực hiện kiểm thử xâm nhập từ bên ngoài (áp dụng đối với hệ thống thông tin cấp độ 4 trở lên)	II.18.2.1. Định kỳ thực hiện kiểm thử xâm nhập từ bên ngoài	Chưa đáp ứng Mức 1.	Đã định kỳ thực hiện kiểm thử xâm nhập từ bên ngoài đối với các ứng dụng, dịch vụ của tổ chức được công khai ra mạng Internet, trong đó: - Cấp độ 4: tối thiểu 01 lần/01 năm; - Cấp độ 5: tối thiểu 01 lần/06 tháng.	Đáp ứng Mức 1 và có cơ chế đo lường, đánh giá tính hiệu quả của hoạt động kiểm thử xâm nhập từ bên ngoài.	Đáp ứng Mức 2 và có cơ chế cải tiến liên tục dựa trên kết quả đánh giá để tối ưu hóa hoạt động kiểm thử xâm nhập từ bên ngoài.	Báo cáo kiểm thử từ bên ngoài
	II.18.3. Khắc phục các tồn tại phát hiện được qua việc kiểm thử xâm nhập	II.18.3.1. Khắc phục các tồn tại phát hiện được qua kiểm thử xâm nhập	Chưa đáp ứng Mức 1.	Đã khắc phục các tồn tại phát hiện được qua kiểm thử xâm nhập dựa trên chính sách của tổ chức về phạm vi và mức độ ưu tiên khắc phục.	Đáp ứng Mức 1 và có cơ chế đo lường, đánh giá tính hiệu quả của hoạt động khắc phục các tồn tại phát hiện được qua kiểm thử xâm nhập.	Đáp ứng Mức 2 và có cơ chế cải tiến liên tục dựa trên kết quả đánh giá để tối ưu hóa hoạt động khắc phục các tồn tại phát hiện được qua kiểm thử xâm nhập.	Biện pháp khắc phục các tồn tại phát hiện được
	II.18.4. Rà soát các biện pháp bảo mật	II.18.4.1. Kiểm tra các biện pháp bảo mật sau mỗi lần thực hiện kiểm thử xâm nhập	Chưa đáp ứng Mức 1.	Thực hiện kiểm tra lại sau kiểm thử nhằm xác nhận các biện pháp bảo mật đã được triển khai và các lỗ hổng đã được khắc phục; có đầy đủ hồ sơ, biên bản và báo cáo xác nhận kết quả kiểm tra lại của đơn vị thực hiện kiểm thử.	Đáp ứng Mức 1 và có cơ chế đo lường, đánh giá tính hiệu quả của hoạt động kiểm tra các biện pháp bảo mật sau mỗi lần thực hiện kiểm thử xâm nhập.	Đáp ứng Mức 2 và có cơ chế cải tiến liên tục dựa trên kết quả đánh giá để tối ưu hóa hoạt động kiểm tra các biện pháp bảo mật sau mỗi lần thực hiện kiểm thử xâm nhập.	Kết quả rà soát các biện pháp bảo mật
	II.18.5. Định kỳ thực hiện kiểm thử xâm nhập từ bên trong (áp dụng đối với hệ thống thông tin cấp độ 4 trở lên)	II.18.5.1. Định kỳ thực hiện kiểm thử xâm nhập từ bên trong	Chưa đáp ứng Mức 1.	Định kỳ thực hiện kiểm thử xâm nhập từ bên trong, áp dụng với các tài nguyên nội bộ trong hệ thống thông tin của tổ chức, trong đó: - Cấp độ 4: tối thiểu 01 lần/01 năm; - Cấp độ 5: tối thiểu 01 lần/06 tháng.	Đáp ứng Mức 1 và có cơ chế đo lường, đánh giá tính hiệu quả của hoạt động kiểm thử xâm nhập từ bên trong.	Đáp ứng Mức 2 và có cơ chế cải tiến liên tục dựa trên kết quả đánh giá để tối ưu hóa hoạt động kiểm thử xâm nhập từ bên trong.	Báo cáo kiểm thử từ bên trong

Phụ lục VII

DANH MỤC TIÊU CHÍ THUỘC NHÓM TIÊU CHÍ PHỤC VỤ CHỈ ĐẠO, ĐIỀU HÀNH CHO HỆ THỐNG THÔNG TIN (NHÓM III)

(Kèm theo Quyết định số 1964/QĐ-TTg ngày 12 tháng 10 năm 2026 của Thủ tướng Chính phủ)

STT	Tiêu chí đánh giá	Phân loại	Số liệu thành phần cần thống kê	Cách xác định giá trị thống kê của Tiêu chí	Căn cứ xác định số liệu
III.1	Tỷ lệ biện pháp xử lý rủi ro được thực hiện đúng hạn theo kế hoạch (%)	Tiêu chí thuận	- Số biện pháp xử lý rủi ro được thực hiện đúng hạn theo kế hoạch. - Tổng số biện pháp xử lý rủi ro trong tất cả kế hoạch.	100*Số biện pháp xử lý rủi ro được thực hiện đúng hạn theo kế hoạch/Tổng số biện pháp xử lý rủi ro trong tất cả kế hoạch.	Căn cứ theo số liệu thống kê của chủ quản hệ thống thông tin.
III.2	Tỷ lệ sự cố an ninh mạng được kiểm soát và xử lý kịp thời trên tổng số lượng sự cố an ninh mạng (%)	Tiêu chí thuận	- Số lượng sự cố an ninh mạng được kiểm soát và xử lý kịp thời. - Tổng số lượng sự cố an ninh mạng xảy ra.	100*Số lượng sự cố an ninh mạng được kiểm soát và xử lý kịp thời/Tổng số lượng sự cố an ninh mạng xảy ra.	Căn cứ theo số liệu thống kê của chủ quản hệ thống thông tin, tuy nhiên không được ít hơn số liệu do cơ quan chức năng ghi nhận.
III.3	Số lượng sự cố an ninh mạng nghiêm trọng xảy ra (số vụ)	Tiêu chí nghịch	- Số lượng sự cố an ninh mạng nghiêm trọng xảy ra.	Số lượng sự cố an ninh mạng nghiêm trọng xảy ra	Căn cứ theo số liệu thống kê của chủ quản hệ thống thông tin, tuy nhiên không được ít hơn số liệu do cơ quan chức năng ghi nhận.
III.4	Số bản ghi dữ liệu cá nhân của công dân bị lộ lọt (số bản ghi)	Tiêu chí nghịch	- Số bản ghi dữ liệu cá nhân của công dân bị lộ lọt.	Số bản ghi dữ liệu cá nhân của công dân bị lộ lọt.	Căn cứ theo số liệu thống kê của chủ quản hệ thống thông tin, tuy nhiên không được ít hơn số liệu do cơ quan chức năng ghi nhận.
III.5	Số Gigabyte dữ liệu bị lộ lọt (GB)	Tiêu chí nghịch	- Số Gigabyte dữ liệu bị lộ lọt.	Số Gigabyte dữ liệu bị lộ lọt.	Căn cứ theo số liệu thống kê của chủ quản hệ thống thông tin, tuy nhiên không được ít hơn số liệu do cơ quan chức năng ghi nhận.
III.6	Số Gigabyte dữ liệu bị mất, mã hoá (GB)	Tiêu chí nghịch	- Số Gigabyte dữ liệu bị mất, mã hoá.	Số Gigabyte dữ liệu bị mất, mã hoá.	Căn cứ theo số liệu thống kê của chủ quản hệ thống thông tin, tuy nhiên không được ít hơn số liệu do cơ quan chức năng ghi nhận.

III.7	Số vụ lộ bí mật nhà nước trên không gian mạng do sự cố an ninh mạng gây ra (vụ)	Tiêu chí nghịch	- Số vụ lộ bí mật nhà nước trên không gian mạng do sự cố an ninh mạng gây ra	Số vụ lộ bí mật nhà nước trên không gian mạng do sự cố an ninh mạng gây ra	Căn cứ theo số liệu thống kê của chủ quản hệ thống thông tin, tuy nhiên không được ít hơn số liệu do cơ quan chức năng ghi nhận.
III.8	Số đầu tài liệu bí mật nhà nước bị đăng tải, truyền đưa trên không gian mạng do sự cố an ninh mạng gây ra (tài liệu)	Tiêu chí nghịch	- Số đầu tài liệu bí mật nhà nước bị đăng tải, truyền đưa trên không gian mạng do sự cố an ninh mạng gây ra.	Số đầu tài liệu bí mật nhà nước bị đăng tải, truyền đưa trên không gian mạng do sự cố an ninh mạng gây ra.	Căn cứ theo số liệu thống kê của chủ quản hệ thống thông tin, tuy nhiên không được ít hơn số liệu do cơ quan chức năng ghi nhận.
III.9	Thiệt hại tài chính do các sự cố an ninh mạng gây ra trên tổng ngân sách chi cho công tác bảo đảm an ninh mạng (%)	Tiêu chí nghịch	- Thiệt hại tài chính do các sự cố an ninh mạng gây ra. - Tổng ngân sách chi cho công tác bảo đảm an ninh mạng.	100*Thiệt hại tài chính do các sự cố an ninh mạng gây ra/Tổng ngân sách chi cho công tác bảo đảm an ninh mạng.	Bao gồm: chi phí cho điều tra, ứng cứu sự cố, khôi phục hệ thống, khôi phục dữ liệu, thuê chuyên gia, dịch vụ hỗ trợ, mua sắm thiết bị, phần mềm thay thế, các khoản đền bù hợp đồng hoặc bị phạt tiền. Không bao gồm: thiệt hại uy tín, thiệt hại thương hiệu, thiệt hại cơ hội kinh doanh, các khoản ước tính không có căn cứ chứng minh.