Phụ lục V

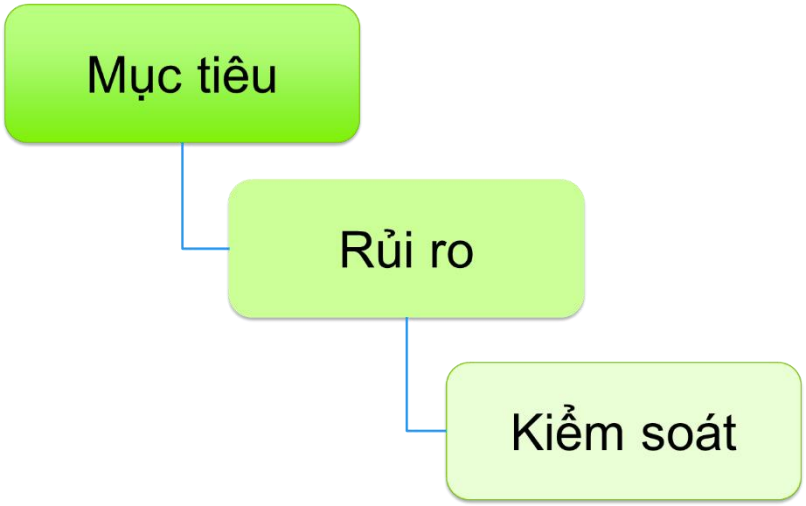
MÔ HÌNH THAM CHIẾU AN TOÀN THÔNG TIN MẠNG, AN NINH MẠNG (SRM)

I. GIỚI THIỆU

Mô hình tham chiếu An toàn thông tin mạng, an ninh mạng (Security Reference Model, viết tắt là SRM) cung cấp một Khung mô tả các thành phần bảo đảm an toàn thông tin mạng, an ninh mạng cần triển khai áp dụng khi phát triển Chính phủ điện tử hướng tới Chính phủ số. Mô hình tham chiếu an toàn thông tin mạng, an ninh mạng là cơ sở để xây dựng Kiến trúc an toàn thông tin mạng, an ninh mạng.

II. CẤU TRÚC MÔ HÌNH THAM CHIẾU AN TOÀN THÔNG TIN MẠNG, AN NINH MẠNG

SRM xây dựng hệ thống an toàn thông tin mạng, an ninh mạng thống nhất thông qua thành phần: Mục tiêu, Rủi ro và Kiểm soát. Các thành phần này sau đó được chia thành 06 hợp phần chi tiết. Mỗi nội dung này phải được giải quyết ở cấp độ tổ chức và hệ thống.



Hình 1. Cấu trúc của mô hình an toàn thông tin mạng, an ninh mạng

Mục tiêu: Các mục tiêu bảo đảm an toàn thông tin mạng, an ninh mạng đối với các hệ thống thành phần trong Khung kiến trúc Chính phủ số Việt Nam. Cụ thể, Hệ thống thông tin cần được thực hiện bảo vệ theo quy định của pháp luật căn cứ vào cấp độ an toàn của hệ thống thông tin, yêu cầu an toàn tối thiểu và phương án tổ chức thực thi.

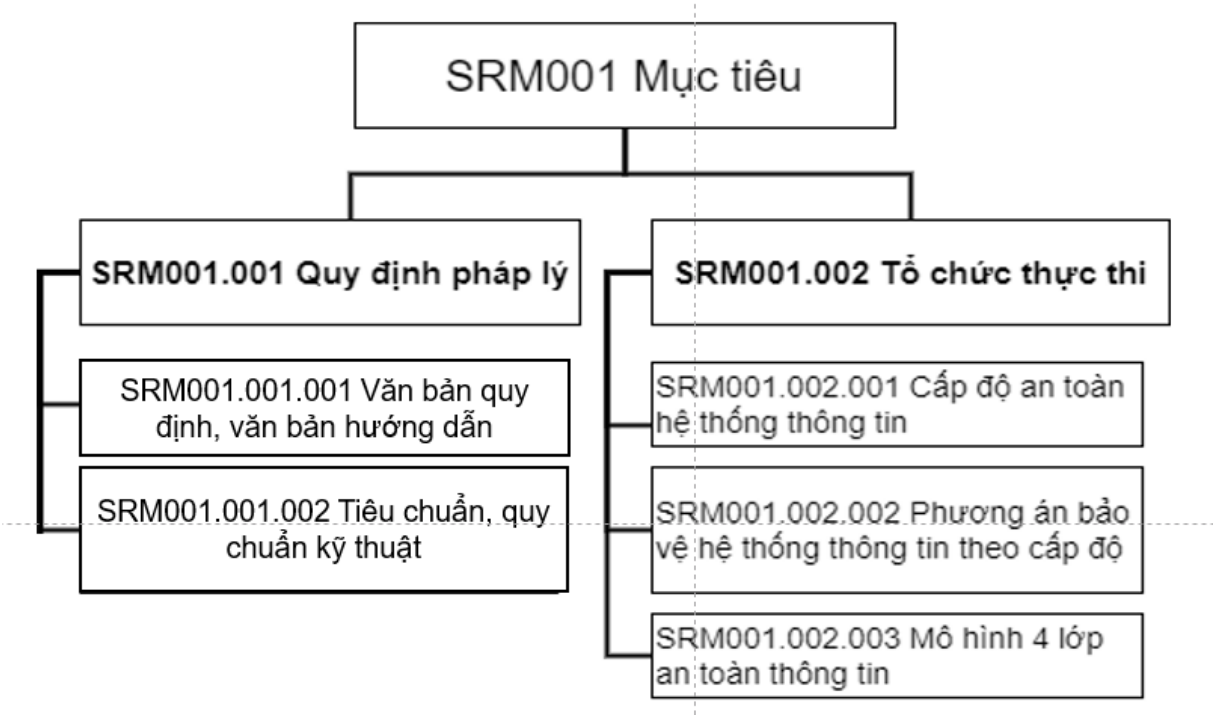
Rủi ro: Các nguy cơ, rủi ro mất an toàn thông tin mạng, an ninh mạng và biện pháp kiểm soát. Cụ thể, các hệ thống thông tin cần được kiểm tra, đánh giá, xác định và quản lý các rủi ro; các nguy cơ, rủi ro đối với hệ thống cần có biện pháp kiểm soát để giảm thiểu mức độ rủi ro thông qua phương án bảo vệ theo cấp độ; biện pháp kiểm tra, đánh giá, giám sát an toàn thông tin mạng, an ninh mạng; phương án ứng cứu, xử lý sự cố.

Kiểm soát: Các biện pháp kiểm soát, đánh giá sự tuân thủ. Cụ thể, việc thực thi bảo vệ các hệ thống thông tin cần được kiểm soát sự tuân thủ quy định của pháp luật và kiểm soát hiệu quả của phương án đảm bảo an toàn hệ thống thông tin theo cấp độ.

III. PHÂN LOẠI

1. Mục tiêu (SRM001)

SRM001 bảo đảm an toàn thông tin mạng, an ninh mạng đối với các hệ thống thành phần trong Khung kiến trúc Chính phủ số Việt nam được xác định là việc thực hiện bảo vệ hệ thống thông tin tuân thủ các quy định của pháp luật, căn cứ vào cấp độ an toàn của hệ thống thông tin, yêu cầu an toàn tối thiểu và phương án bảo vệ. Trên cơ sở đó, SRM001 bao gồm 02 hợp phần: (1) Quy định pháp lý và (2) Tổ chức thực thi.



Hình 2. Cấu trúc phân cấp Mục tiêu

a) Quy định pháp lý (SRM001.001)

SRM001.001 bao gồm các hệ thống các văn bản pháp luật, văn bản hướng dẫn về bảo đảm an toàn thông tin mạng, an ninh mạng cùng hệ thống các tiêu chuẩn về an toàn thông tin mạng, an ninh mạng. Cụ thể như sau:

STT	Ngữ cảnh	Mô tả
1	SRM001.001.001 Văn bản quy định, văn bản hướng dẫn	Bao gồm nhưng không giới hạn các Luật sau: - Luật An toàn thông tin mạng năm 2015; - Luật An ninh mạng năm 2018; - Luật Giao dịch điện tử năm 2023;

STT	Ngữ cảnh	Mô tả
		- Luật Dữ liệu năm 2024; - Luật Bảo vệ bí mật nhà nước năm 2018… Ngoài ra, bao gồm các Nghị định, Thông tư, Tiêu chuẩn về an toàn thông tin mạng, an ninh mạng mà các cơ quan nhà nước và các tổ chức, cá nhân có liên quan phải áp dụng hoặc khuyến nghị áp dụng theo quy định pháp luật.
2	SRM001.001.002 Tiêu chuẩn, quy chuẩn kỹ thuật	Bao gồm nhưng không giới hạn các tiêu chuẩn sau: (1) TCVN 11930:2017 Công nghệ thông tin - Các kỹ thuật an toàn - Yêu cầu cơ bản về an toàn thông tin theo cấp độ. (2) TCVN ISO/IEC 27001:2019 Công nghệ thông tin - Hệ thống quản lý an toàn thông tin - Các yêu cầu. (3) TCVN ISO/IEC 27002:2020 Công nghệ thông tin-Các kỹ thuật an toàn - Quy tắc thực hành Quản lý an toàn thông tin. (4) TCVN 8709-1:2011 ISO/IEC 15408 -1:2009 Công nghệ thông tin- Các kỹ thuật an toàn - Các tiêu chí đánh giá an toàn CNTT - Phần 1: Giới thiệu và mô hình tổng quát. (5) TCVN 8709-2:2011 ISO/IEC 15408 -2:2008 Công nghệ thông tin - Các kỹ thuật an toàn - Các tiêu chí đánh giá an toàn CNTT - Phần 2: Các thành phần chức năng an toàn. (6) TCVN 8709-3:2011 ISO/IEC 15408 -3:2008 Công nghệ thông tin- Các kỹ thuật an toàn - Các tiêu chí đánh giá an toàn CNTT- Phần 3: Các thành phần đảm bảo an toàn. (7) TCVN 10295:2014 ISO/IEC 27005:2011 Công nghệ thông tin - Các kỹ thuật an toàn -Quản lý rủi ro an toàn thông tin. (8) TCVN 10541:2014 ISO/IEC 27003:2010 Công nghệ thông tin - Các kỹ thuật an toàn - Hướng dẫn triển khai hệ thống quản lý an toàn thông tin. (9) TCVN 10543:2014 ISO/IEC 27010:2012 Công nghệ thông tin - Các kỹ thuật an toàn - Quản lý an toàn trao đổi thông tin liên tổ chức, liên ngành. (10) TCVN 9801-3:2014 ISO/IEC 27033-3:2010 Công nghệ thông tin - Kỹ thuật an toàn - An toàn mạng - Phần 3: Các kịch bản kết nối mạng tham chiếu - Nguy cơ, kỹ thuật thiết kế và các vấn đề kiểm soát.

STT	Ngữ cảnh	Mô tả
		(11) TCVN 9801-2:2015 Công nghệ thông tin - Các kỹ thuật an toàn - An toàn mạng - Phần 2: Hướng dẫn thiết kế và triển khai an toàn mạng. (12) TCVN 11238:2015 Công nghệ thông tin - Các kỹ thuật an toàn - Hệ thống quản lý an toàn thông tin - Tổng quan và từ vựng. (13) TCVN 11239:2015 Công nghệ thông tin - Các kỹ thuật an toàn - Quản lý sự cố an toàn thông tin. (14) TCVN 11386:2016 Công nghệ thông tin - Các kỹ thuật an toàn - Phương pháp đánh giá an toàn công nghệ thông tin. (15) TCVN 11393-1:2016 ISO/IEC 13888-1:2009 Công nghệ thông tin - Các kỹ thuật an toàn - Chống chối bỏ - Phần 1: Tổng quan. (16) TCVN 11393-2:2016 ISO/IEC 13888-2:2009 Công nghệ thông tin - Các kỹ thuật an toàn - Chống chối bỏ - Phần 2: Các cơ chế sử dụng kỹ thuật đối xứng. (17) TCVN 11393-3:2016 ISO/IEC 13888-3:2009 Công nghệ thông tin - Các kỹ thuật an toàn - Chống chối bỏ - Phần 3: Các cơ chế sử dụng kỹ thuật bất đối xứng.

b) Tổ chức thực thi (SRM001.002)

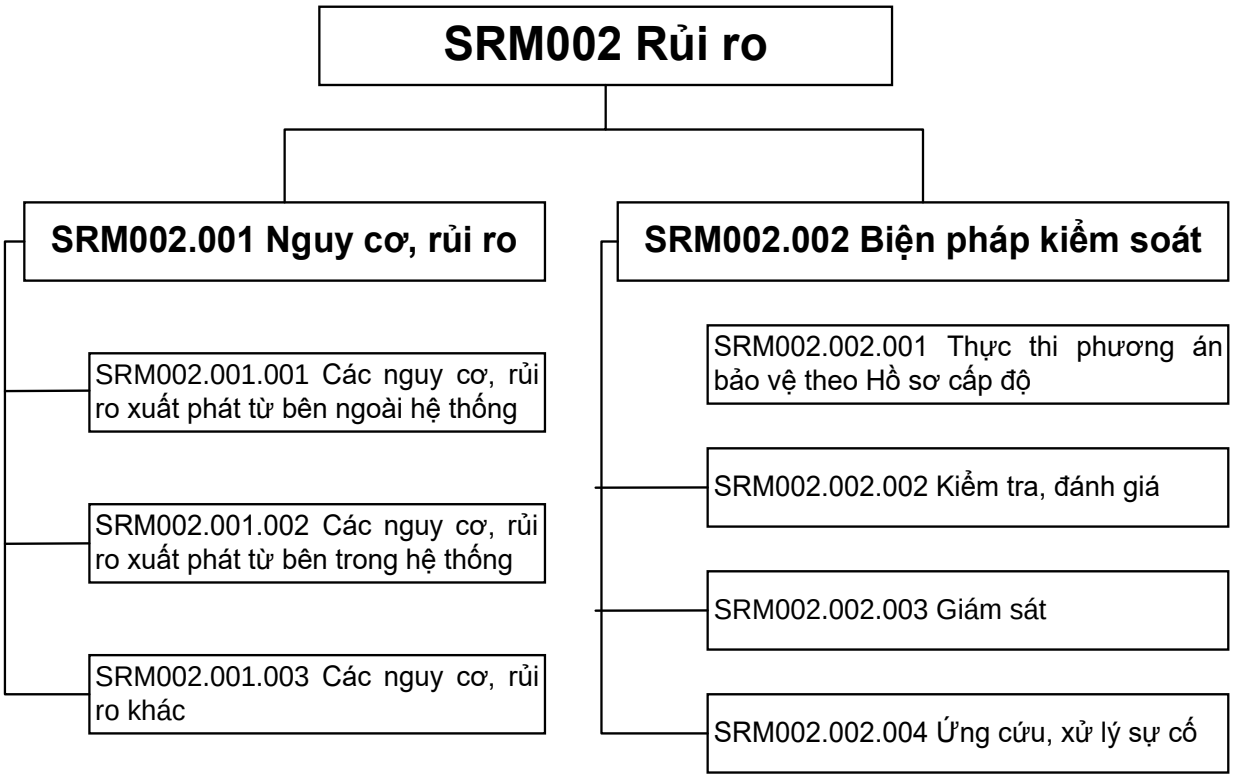
Tổ chức thực thi SRM001.002 được mô tả như trong bảng dưới đây.

STT	Ngữ cảnh	Mô tả
1	SRM001.002.001 Cấp độ an toàn của hệ thống thông tin	Tài liệu mô tả tổng quan, thiết kế liên quan đến hệ thống thông tin, đưa ra các căn cứ xác định cấp độ an toàn thông tin mạng, an ninh mạng của các hệ thống thông tin.
2	SRM001.002.002 Phương án bảo vệ hệ thống thông tin theo cấp độ	Tài liệu mô tả về các phương án bảo đảm an toàn căn cứ theo các tiêu chí, yêu cầu quản lý và kỹ thuật theo các quy định bảo đảm an toàn thông tin mạng, an ninh mạng cho các hệ thống thông tin theo cấp độ.
3	SRM001.002.003 Mô hình 4 lớp	Cơ quan, tổ chức triển khai bảo đảm an toàn thông tin mạng, an ninh mạng cho các HTTT theo mô hình "4 lớp", gồm: Lớp 1 - Lực lượng tại chỗ; Lớp 2 - Tổ chức hoặc doanh nghiệp giám sát, bảo vệ chuyên nghiệp (Lực lượng giám sát, bảo vệ chuyên nghiệp); Lớp 3 - Tổ chức hoặc doanh nghiệp độc lập kiểm tra, đánh

STT	Ngữ cảnh	Mô tả
		giá định kỳ (Lực lượng kiểm tra, đánh giá độc lập); Lớp 4 - Kết nối, chia sẻ thông tin với hệ thống giám sát quốc gia (SOC Quốc gia).

2. Rủi ro (SRM002)

Nội dung Rủi ro mô tả các nguy cơ, rủi ro mất an toàn thông tin mạng, an ninh mạng và biện pháp kiểm soát.



Hình 3. Cấu trúc phân cấp Rủi ro

a) Nguy cơ, rủi ro (SRM002.001)

SRM002.001 đưa ra các nguy cơ, rủi ro mất an toàn thông tin mạng, an ninh mạng đối với hệ thống. Các nguy cơ, rủi ro có thể được xác định từ các yếu tố bên trong hoặc từ các yếu tố bên ngoài tác động vào hệ thống. SRM002.001 bao gồm các hợp phần sau:

STT	Ngữ cảnh	Mô tả
1	SRM002.001.001 Các nguy cơ, rủi ro xuất phát từ bên ngoài hệ thống	Các nguy cơ, rủi ro mất an toàn thông tin mạng, an ninh mạng xuất phát từ bên ngoài hệ thống như tấn công có chủ đích (APT), DoS/DDoS, tấn công Deface, tấn công khai thác điểm yếu lỗ hổng bảo mật… từ bên ngoài hoặc các yếu tố khách quan do thiên nhiên tác động như động đất, bão, lũ lụt, cháy nổ, sét …
2	SRM002.001.002 Các nguy cơ, rủi ro xuất phát từ bên trong hệ thống	Các nguy cơ, rủi ro mất an toàn thông tin mạng, an ninh mạng xuất phát từ bên trong hệ thống như: Tấn công mã độc, tấn công nghe lén đánh cắp, rủi ro về dữ liệu và quyền riêng tư (lộ lọt, rò rỉ hoặc đánh cắp dữ liệu, truy cập trái phép,

STT	Ngữ cảnh	Mô tả
		sử dụng dữ liệu sai mục đích…), tấn công thông qua môi trường vật lý…
3	SRM002.001.003 Các nguy cơ, rủi ro khác	Các nguy cơ, rủi ro mất an toàn thông tin mạng, an ninh mạng khác theo đặc trưng của từng hệ thống cụ thể (ví dụ: bảo mật yếu trong các ứng dụng, phần mềm, thiết kế hệ thống không an toàn, thiếu kiểm soát…; rủi ro từ công nghệ (tấn công vào hệ thống trí tuệ nhân tạo và dữ liệu lớn, nguy cơ từ IoT…); rủi ro thiếu chính sách và nhận thức về an thoàn tông tin mạng, an ninh mạng, giả mạo chữ ký số…

b) Biện pháp kiểm soát (SRM002.002)

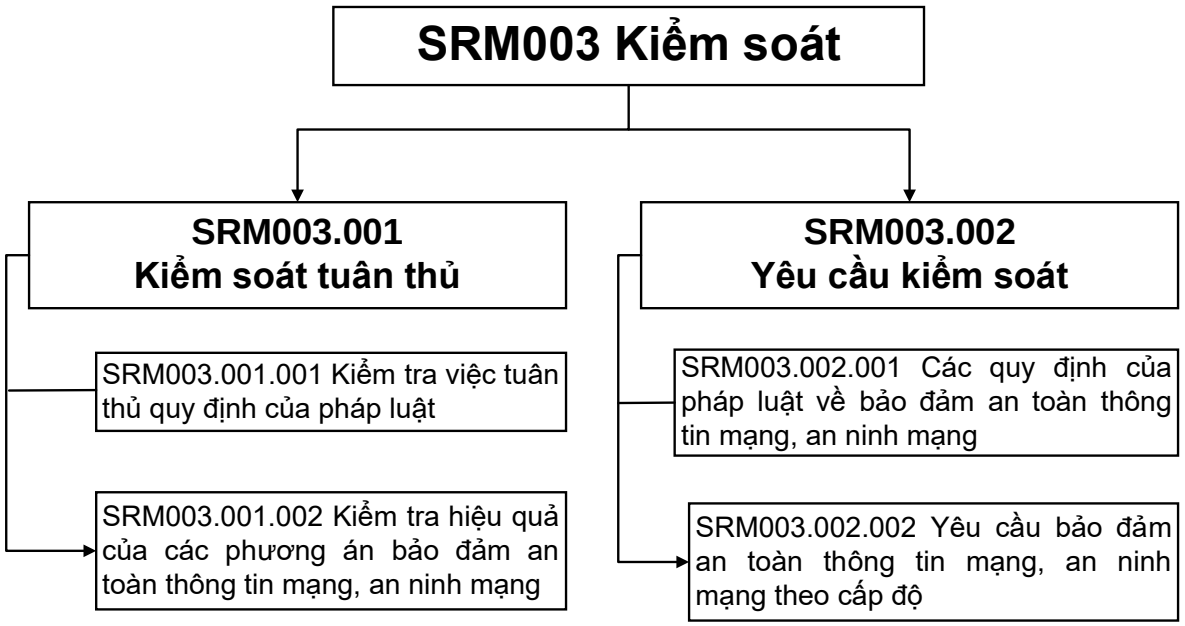
SRM002.002 Biện pháp kiểm soát là các biện pháp quản lý và kỹ thuật được sử dụng để giảm thiểu các nguy cơ, rủi ro mất an toàn thông tin mạng, an ninh mạng đối với hệ thống. SRM002.002 bao gồm các hợp phần sau:

STT	Ngữ cảnh	Mô tả
1	SRM002.002.001 Thực thi phương án bảo vệ theo Hồ sơ cấp độ	Triển khai các phương án bảo đảm an toàn các hệ thống thông tin, hệ thống thông tin quan trọng về an ninh quốc gia theo các quy định pháp luật, theo Hồ sơ cấp độ được phê duyệt để đáp ứng các yêu cầu cơ bản về quản lý và kỹ thuật.
2	SRM002.002.002 Kiểm tra, đánh giá	Việc thực hiện kiểm tra, đánh giá an toàn thông tin mạng, an ninh mạng như mã hóa dữ liệu (cơ yếu nếu có), thử nghiệm xâm nhập hệ thống nhằm kiểm tra mức độ kiểm soát truy cập và xác thực) hoặc phát hiện mã độc, lỗ hổng (lỗi phần mềm, chưa cập nhật bản vá, lỗi bảo mật ứng dụng…), lộ lọt rò rỉ dữ liệu, và các nguy cơ, rủi ro khác (kiến thức, nhận thức về an toàn thông tin mạng, an ninh mạng chưa cao) có thể xảy ra làm mất bảo đảm an toàn thông tin mạng, an ninh mạng của các hệ thống thông tin.
3	SRM002.002.003 Giám sát	Triển khai phương án giám sát an toàn thông tin mạng, an ninh mạng nhằm phát hiện sớm nhất các cuộc tấn công mạng đối với hệ thống thông tin của các cơ quan nhà nước, đồng thời, chia sẻ thông tin, dữ liệu giám sát hoặc dữ liệu liên quan theo quy định hoặc trong trường hợp cần thiết, cần hỗ trợ.

STT	Ngữ cảnh	Mô tả
4	SRM002.002.004 Ứng cứu, xử lý sự cố	Triển khai các phương án ứng cứu, xử lý sự cố nhằm bảo đảm hệ thống có thể khôi phục hoạt động bình thường sớm nhất có thể sau sự cố (như sao lưu, lưu trữ, phục hồi...).

3. Kiểm soát (SRM003)

SRM003 bao gồm các biện pháp đánh giá sự tuân thủ và kiểm soát an toàn thông tin mạng, an ninh mạng cho các hệ thống thông tin trong quá trình xây dựng, quản lý, vận hành và gỡ bỏ theo quy định của pháp luật.



Hình 4. Cấu trúc phân cấp Kiểm soát

Các kiểm soát thuộc SRM003 được liệt kê dưới đây:

a) Kiểm soát tuân thủ (SRM003.001)

STT	Ngữ cảnh	Mô tả
1	SRM003.001.001 Kiểm tra việc tuân thủ quy định của pháp luật	Kiểm tra việc thực thi bảo vệ hệ thống thông tin của cơ quan, tổ chức, hệ thống thông tin quan trọng về an ninh quốc gia có tuân thủ các quy định của pháp luật về bảo đảm an toàn thông tin mạng, an ninh mạng hay không (bao gồm các quy định của pháp luật về bảo đảm an toàn hệ thống thông tin theo cấp độ và các quy định khác liên quan).
2	SRM003.001.002 Kiểm tra hiệu quả của các phương án bảo đảm an toàn	Đánh giá việc triển khai các phương án bảo đảm an toàn thông tin mạng, an ninh mạng theo phương án trong Hồ sơ đề xuất cấp độ đã được phê duyệt; đánh giá việc triển khai

STT	Ngữ cảnh	Mô tả
	thông tin mạng, an ninh mạng	các phương án bảo đảm an toàn thông tin mạng, an ninh mạng theo hồ sơ đề xuất về hệ thống thông tin quan trọng về an ninh quốc gia theo quy định pháp luật; đánh giá hiệu quả của các biện pháp kiểm soát rủi ro.

b) Yêu cầu kiểm soát (SRM003.002)

Yêu cầu kiểm soát xem xét các hoạt động cụ thể, triển khai và quy trình kỹ thuật để giảm thiểu hoặc loại bỏ lỗ hổng, điểm yếu đã biết. Danh mục yêu cầu kiểm soát dựa vào biện pháp kiểm soát để chi tiết thực thi, triển khai các phương án bảo đảm an toàn hệ thống thông tin theo quy định của pháp luật.

Các nội dung thuộc SRM003.002 được liệt kê trong bảng dưới đây:

STT	Ngữ cảnh	Mô tả
1	SRM003.002.001 Các quy định của pháp luật về bảo đảm an toàn thông tin mạng, an ninh mạng	Yêu cầu kiểm tra, đánh giá định kỳ có hệ thống sự phù hợp, mức độ đáp ứng về bảo đảm an toàn thông tin mạng, an ninh mạng cho các HTTT so với các quy định pháp luật.
2	SRM003.002.002 Yêu cầu bảo đảm an toàn thông tin mạng, an ninh mạng theo cấp độ	Yêu cầu kiểm tra, đánh giá định kỳ, thường xuyên, liên tục, có hệ thống mức độ đáp ứng các yêu cầu về cấp độ an toàn của hệ thống theo các tiêu chuẩn, quy chuẩn quốc gia về bảo đảm an toàn thông tin mạng, an ninh mạng.