Phụ lục V

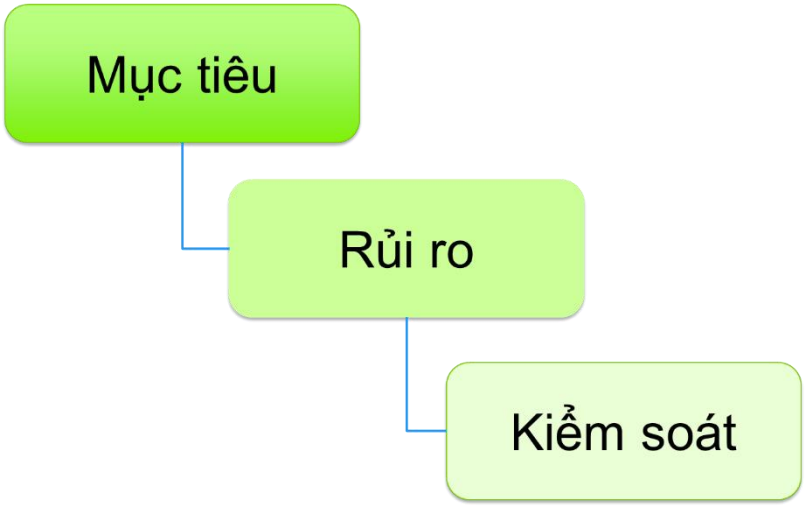
MÔ HÌNH THAM CHIẾU AN TOÀN THÔNG TIN (SRM)

I. GIỚI THIỆU

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

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

SRM xây dựng hệ thống an toàn thông tin 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 phân tầng của mô hình an toàn thông tin

Mục tiêu: Các mục tiêu bảo đảm an toàn thông tin đối với các hệ thống thành phần trong Khung CPĐT. 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 bảo vệ.

Rủi ro: Các nguy cơ, rủi ro mất an toàn thông tin 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.

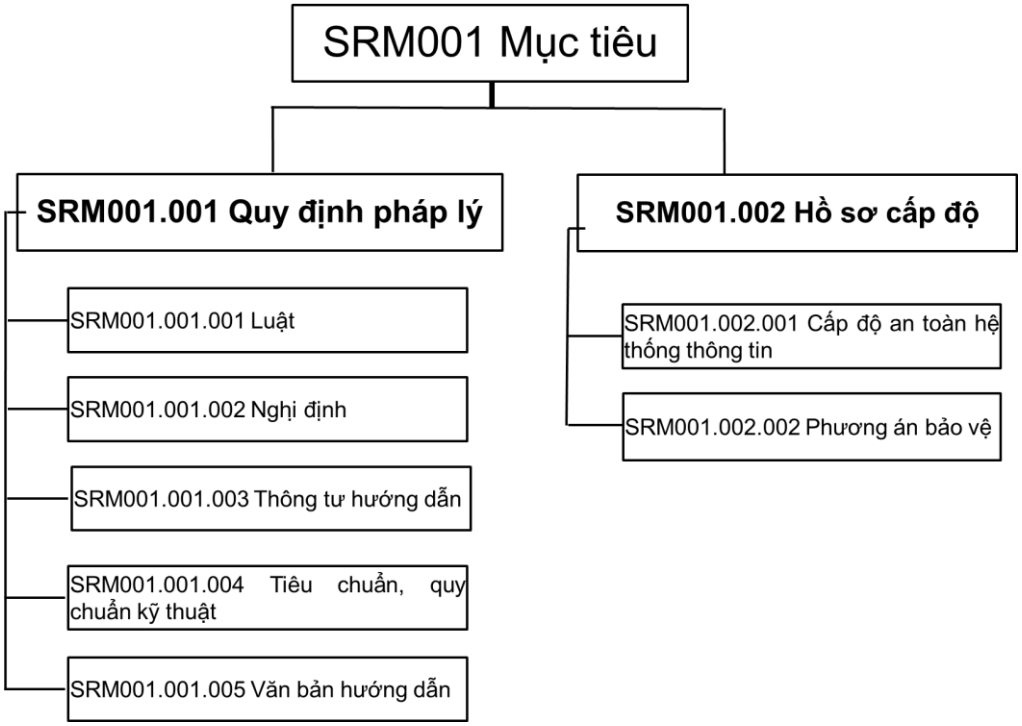
Kiểm soát: Các biện pháp kiểm soát, đánh giá sự tuân thủ. Cụ thể, việc thực thi bảo vệ các hệ thống thông tin cần được kiểm soát sự tuân thủ quy định của pháp luật và đánh giá hiệu quả của phương án bảo vệ.

III. PHÂN LOẠI

1. 1. Mục tiêu (SRM001)

SRM001 bảo đảm an toàn thông tin đối với các hệ thống thành phần trong Kiến trúc Chính phủ điện tử 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) Hồ sơ cấp độ.



Hình 2. Cấu trúc phân cấp Mụctiêu

Hợp phần Mục tiêu về Quy định pháp lý và Hồ sơ cấp độ được liệt kê dưới đây:

a) Quy định pháp lý (SRM001.001)

SRM001.001 bao gồm các hệ thống các văn bản quy phạm pháp luật về bảo đảm an toàn thông tin mạng, các văn bản hướng dẫn thực thi cụ thể và hệ thống các tiêu chuẩn về an toàn thông tin.

Khi xây dựng Kiến trúc Chính phủ điện tử cấp bộ, Kiến trúc Chính quyền điện tử cấp tỉnh, thành phần tham chiếu này cần chi tiết theo thiết kế thực tế.

Mô tả chi tiết của hợp phần Quy định pháp lý được liệt kê trong bảng dưới đây:

STT	Ngữ cảnh	Mô tả
1	SRM001.001.001 Luật	Bao gồm nhưng không giới hạn các Luậtsau: - Luật An toàn thông tin mạng năm 2015.
2	SRM001.001.002 Nghị định	Bao gồm nhưng không giới hạn các Nghị định hiện hành bao gồm: - Nghị định số 85/2016/NĐ-CP ngày 01/7/2016 của Chính phủ về đảm bảo an toàn thông tin hệ thống theo cấp độ
3	SRM001.001.003 Thông tư hướng dẫn	Bao gồm nhưng không giới hạn các Thông tư sau: - Thông tư số 03/2017/TT-BTTTT ngày

		24/4/2017 của Bộ trưởng Bộ Thông tin và Truyền thông quy định chi tiết và hướng dẫn một số điều của Nghị định số 85/2016/NĐ-CP ngày 01/7/2016 củaChính phủ về đảm bảo an toàn thông tin hệ thống theo cấp độ; - Thông tư số 20/2017/TT-BTTTT, ngày 12/9/2017 của Bộ Thông tin và Truyền thông quy định về điều phối, ứng cứu sự cố an toàn thông tin mạng trên toàn quốc; - Thông tư số 27/2017/TT-BTTTT, ngày 20/10/2017 của Bộ Thông tin và Truyền thông quy định về quản lý, vận hành, kết nối, sử dụng và bảo đảm an toàn thông tin trên mạng truyền số liệu chuyên dùng của các cơ quan Đảng, Nhà nước; Thông tư số 12/2019/TT-BTTTT ngày 5/11/2019 sửa đổi Thông tư 27/2017/TT-BTTTT. - Thông tư số 31/2017/TT-BTTTT ngày 15/11/2017 của Bộ Thông tin và Truyền thôn quy định hoạt động giám sát an toàn hệ thống thông tin.
4	SRM001.001.004 Tiêu chuẩn, quy chuẩnkỹ thuật	Bao gồm nhưng không giới hạn các tiêu chuẩn sau: (1) TCVN 11930:2017/BTTTT 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 27001:2009 Công nghệ thông tin - Hệ thống quản lý an toàn thông tin – Các yêu cầu. (3) TCVN ISO/IEC 27002:2011 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. (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.
5	SRM001.001.005 Văn	Đề cập các nghị định hướng dẫn các luật về

	bản hướng dẫn	an toàn thông tin mạng được áp dụng trong các cơ quan Chính phủ Việt Nam. Các văn bản hướng dẫn hiện hành bao gồm: - Văn bản số 2132/BTTTT-VNCERT ngày 18/07/2011 của Bộ Thông tin và Truyền thông về việc Hướng dẫn đảm bảo an toàn thông tin cho các Cổng/Trang thông tin điện tử. - Văn bản số 430/BTTTT-CATTT ngày 09/02/2015 của Bộ Thông tin và Truyền thông về việc Hướng dẫn bảo đảm an toàn thông tin cho hệ thống thư điện tử của cơ quan, tổ chức Nhà nước. - Văn bản số 2290/BTTTT-CATTTTngày 17/02/2018 của Bộ TTTT về việc Hướng dẫn kết nối, chia sẻ thông tin về mã độc giữa các hệ thống kỹ thuật.

b) Hồ sơ cấp độ (SRM001.002)

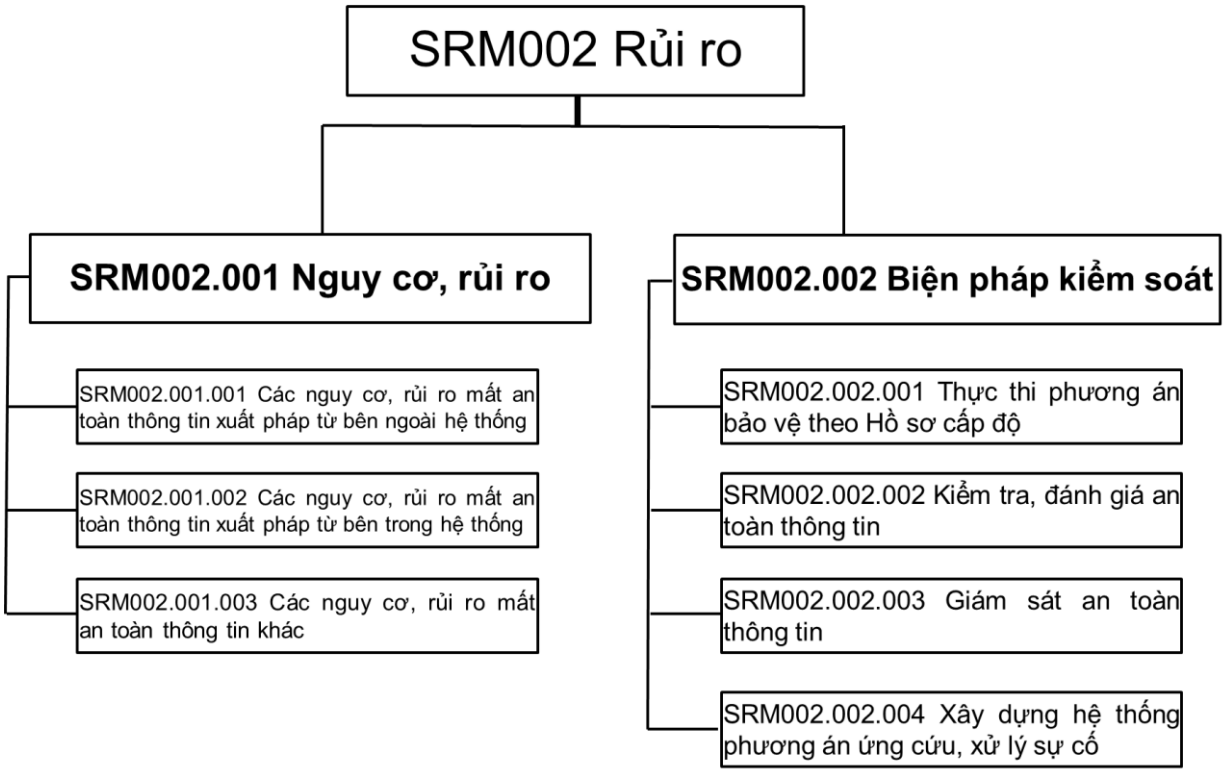
Hồ sơ cấp độ bao gồm: (1) Cấp độ an toàn của hệ thống thông tin và phương án bảo vệ. Trong đó, cấp độ an toàn của hệ thống thông tin được xác định dựa vào mức độ quan trọng của hệ thống thông tin đó và ảnh hưởng của hệ thống thông tin đó khi bị phá hoại; (2) Phương án bảo vệ bao gồm các phươn án về kỹ thuật và phương án về quản lý. Trong đó, phương án kỹ thuật nhằm bảo đảm an toàn thông tin cho hệ thống trong việc thiết kế, thiết lập hệ thống; phương án quản lý nhằm bảo đảm an toàn thông tin trong quá trình quản lý vận hành và khai thác hệ thống.

Mô tả về các hợp phần thuộc SRM001.002 được liệt kê 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 của hệ thống
2	SRM001.002.002 Phương án bảo vệ	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 hệ thống thông tin theo cấp độ.

2. Rủi ro (SRM002)

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



Hình 3. Cấutrúc phân cấpRủi ro

Hợp phần chi tiế tRủi ro được liệt kê dưới đây:

a) Nguy cơ, rủi ro (SRM002.001)

SRM002.001 đưa ra các nguy cơ, rủi ro mất an toàn thông tin 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. SRM002.001bao gồm các hợp phần sau:

STT	Ngữ cảnh	Mô tả
1	SRM002.001.001 Các nguy cơ, rủi ro mất an toàn thông tin xuất pháp từ bên ngoài hệ thống	Các nguy cơ, rủi ro mất an toàn thông tin xuất pháp từ bên ngoài hệ thống như: Tấn công DoS/DDoS, tấn công Deface, tấn công khai thác điểm yếu lỗ hổng bảo mật từ bên ngoài…
2	SRM002.001.002 Các nguy cơ, rủi ro mất an toàn thông tin xuất pháp từ bên trong hệ thống.	Các nguy cơ, rủi ro mất an toàn thông tin xuất pháp từ bên trong hệ thống như: Tấn công mã độc, tấn công nghe lén đánh cắp, lộ lọt thông tin, tấn công thông qua môi trường vật lý…
3	SRM002.001.003 Các nguy cơ, rủi ro mất an toàn thông tin khác	Các nguy cơ, rủi ro mất an toàn thông tin khác theo đặc trưng của từng hệ thống cụ thể.

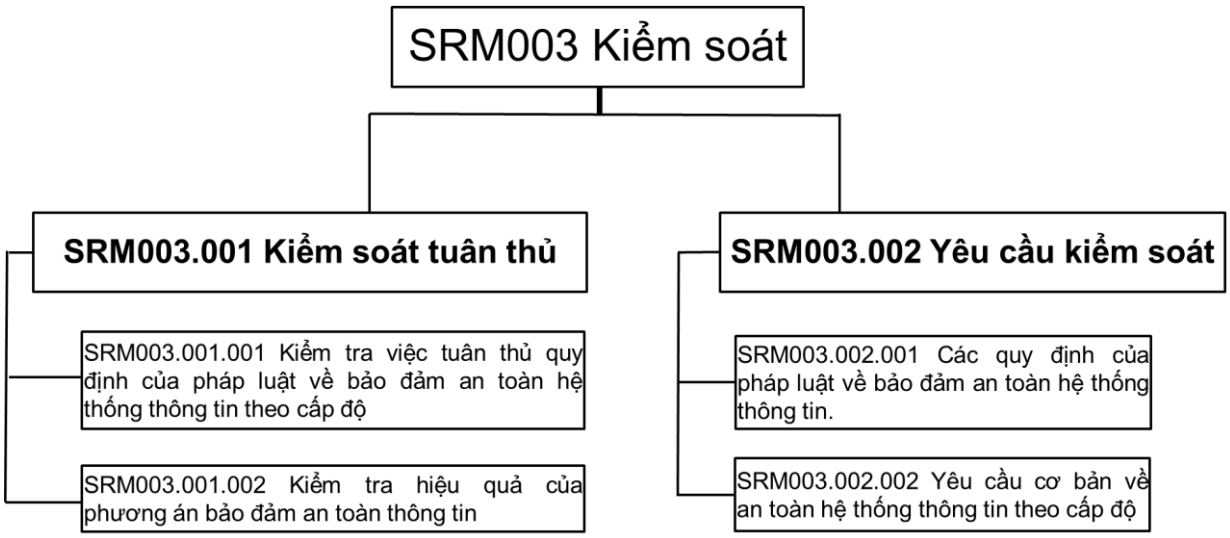
b) Biện pháp kiểm soát (SRM002.002)

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 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 hệ thống thông tin 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 an toàn thông tin	Việc thực hiện kiểm tra, đánh giá an toàn thông tin, thử nghiệm xâm nhập hệ thống nhằm phát hiện mã độc, lỗ hổng, điểm yếu và các nguy cơ, rủi ro mất an toàn thông tin khác có thể xảy ra đối với hệ thống.
3	SRM002.002.003 Giám sát an toàn thông tin	Triển khai phương án giám sát an toàn thông tin nhằm phát hiện sớm nhất các cuộc tấn công mạng đối với hệ thống của mình.
4	SRM002.002.004 Xây dựng hệ thống phương án ứng cứu, xử lý sự cố	Xây dựng hệ thống phương án ứng cứu, xử lý dự cố nhằm bảo đảm hệ thống có thể khôi phục hoạt động bình thường sớm nhất có thể sau sự cố.

3. Kiểm soát (SRM003)

SRM003 bao gồm các biện pháp kiểm soát, đánh giá sự tuân thủ: Việc bảo đảm an toàn cho hệ thống thông tin phải được thực hiện trong các quá trình xây dựng, quản lý vận hành và gỡ bỏ theo quy định của pháp luật.



Hình 4. Cấutrúc phân cấpKiểmsoát

Các kiểm soát thuộc SRM003 được liệt kê dưới đây:

a) Kiểm soát tuân thủ (Ký hiệu/Mã là: SRM003.001)

Kiểm soát tuân thủ bao gồm: (1) Kiểm tra việc tuân thủ quy định của pháp luật về bảo đảm an toàn hệ thống thông tin và (2) Kiểm tra hiệu quả của phương án bảo đảm an toàn thông tin.

STT	Ngữ cảnh	Mô tả
1	SRM003.001.001 Kiểm tra việc tuân thủ quy định của pháp luật về bảo đảm an toàn hệ thống thông tin	Kiểm tra việc thực thi bảo vệ hệ thống thông tin của cơ quan, tổ chức có tuân thủ các quy định của pháp luật về bảo đảm an toàn hệ thống thông tin, 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 phương án bảo đảm an toàn thông tin	Đánh giá việc triển khai các phương án bảo đảm an toàn thông tin theo phương án trong Hồ sơ đề xuất cấp độ đã được phê duyệt; 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 thuộcSRM003.003 Các phân loại kiểm soát 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 hệ thống thông tin	Các quy định của pháp luật về bảo đảm an toàn hệ thống thông tin được mô tả tại SRM001.001 Quy định pháp lý.
2	SRM003.002.002 Yêu cầu cơ bản về an toàn hệ thống thông tin theo cấp độ	Yêu cầu cơ bản về an toàn hệ thống thông tin theo cấp độ bao gồm các yêu cầu về Kỹ thuật và Quản lý theo từng cấp độ an toàn của hệ thống tại tiêu chuẩn quốc gia TCVN 11930:2017 và các tiêu chuẩn khác liên quan.