

**KHUNG KIẾN TRÚC CPĐT VIỆT NAM**  
**Phiên bản 2.0**  
*(dự thảo lần 3)*

Mô hình tham chiếu an toàn thông tin, phiên bản 1.0  
Security Reference Model – SRM, version 1.0

Hà Nội, 5/2019

## MỤC LỤC

|  |           |
|--|-----------|
| <b>1. Mô hình tham chiếu An toàn thông tin mạng (SRM).....</b> | <b>3</b>  |
| <b>1.1. Giới thiệu.....</b>                                    | <b>3</b>  |
| <b>1.2. Cấu trúc.....</b>                                      | <b>3</b>  |
| <b>1.3. SRM001 Mục đích.....</b>                               | <b>4</b>  |
| 1.3.1. SRM001.001 Các điều kiện pháp lý .....                  | 5         |
| 1.3.2. SRM001.002 Hồ sơ rủi ro.....                            | 8         |
| <b>1.4. SRM002 Rủi ro .....</b>                                | <b>9</b>  |
| 1.4.1. SRM002.001 Các quy trình đánh giá rủi ro.....           | 10        |
| 1.4.2. SRM002.002 Làm giảm tác động.....                       | 11        |
| <b>1.5. SRM003 Các kiểm soát.....</b>                          | <b>12</b> |
| 1.5.1. SRM003.001 Sự tuân thủ.....                             | 13        |
| 1.5.2. SRM003.002 Các phân loại kiểm soát .....                | 14        |

## 1. Mô hình tham chiếu An toàn thông tin mạng (SRM)

### 1.1. Giới thiệu

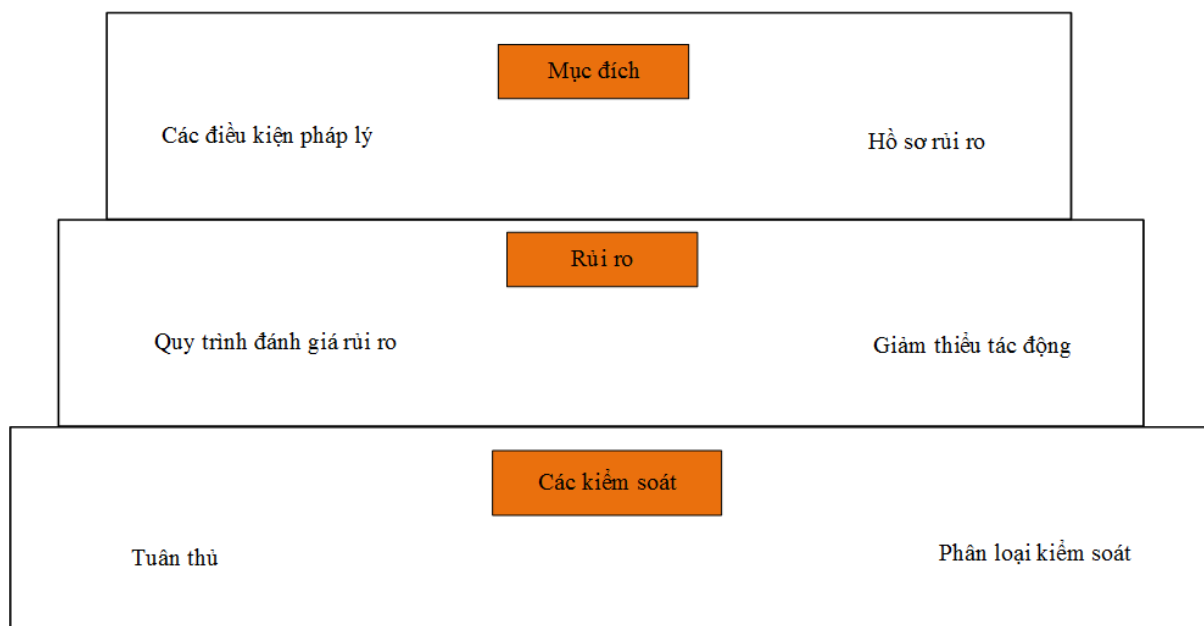
Vấn đề an toàn thông tin mạng là không thể thiếu và có tính xuyên suốt trong tất cả các miền kiến trúc và ở tất cả các cấp của cơ quan, tổ chức. Kết quả, mô hình tham chiếu an toàn thông tin mạng (SRM) phải được đưa vào, xuyên suốt trong trong tất cả các miền kiến trúc của Kiến trúc tổng thể CPĐT Việt Nam. An toàn thông tin mạng phải được xem xét ở các mức độ khác nhau của cơ quan, tổ chức. Quản trị Kiến trúc tổng thể CPĐT là một phương pháp toàn diện để xây dựng các chính sách, tiêu chuẩn, quy chuẩn kỹ thuật về an toàn thông tin mạng.

SRM cho phép kiến trúc sư thực hiện phân lớp hoặc phân loại kiến trúc an toàn thông tin tại tất cả các cấp của kiến trúc CPĐT Việt Nam: Chính phủ, Bộ/tỉnh, ngành/lĩnh vực, hệ thống và ứng dụng. Ở cấp độ cao nhất, SRM được sử dụng để chuyển đổi các luật, các quy định, chính sách và các văn bản liên quan. Ở cấp độ Bộ/tỉnh, ngành/lĩnh vực, các SRM được sử dụng để triển khai, áp dụng các chính sách cụ thể vào cơ chế giám sát bảo mật và đo lường. Ở cấp độ hệ thống, ứng dụng SRM được sử dụng để triển khai, áp dụng cơ chế giám sát vào các hệ thống thiết kế theo yêu cầu cụ thể. Mỗi cấp độ, SRM đóng vai trò quan trọng đối với kiến trúc tổng thể về an toàn thông tin mạng của một tổ chức và/hoặc hệ thống.

### 1.2. Cấu trúc

Mô hình tham chiếu bảo mật (SRM) có ba khu vực: Mục đích, Rủi ro, và Các kiểm soát; chúng được chia thành sáu phân nhóm (hình bên dưới). Mỗi một trong những phân nhóm được ra ở cấp độ cơ quan, tổ chức, và hệ thống. Các SRM sử dụng thông tin từ mục đích và rủi ro ở mỗi cấp độ của các tổ chức để tìm kiếm và phân loại các giám sát phù hợp để đảm bảo bảo mật môi trường...

Cấu trúc mức cao của SRM được hiển thị bên dưới:



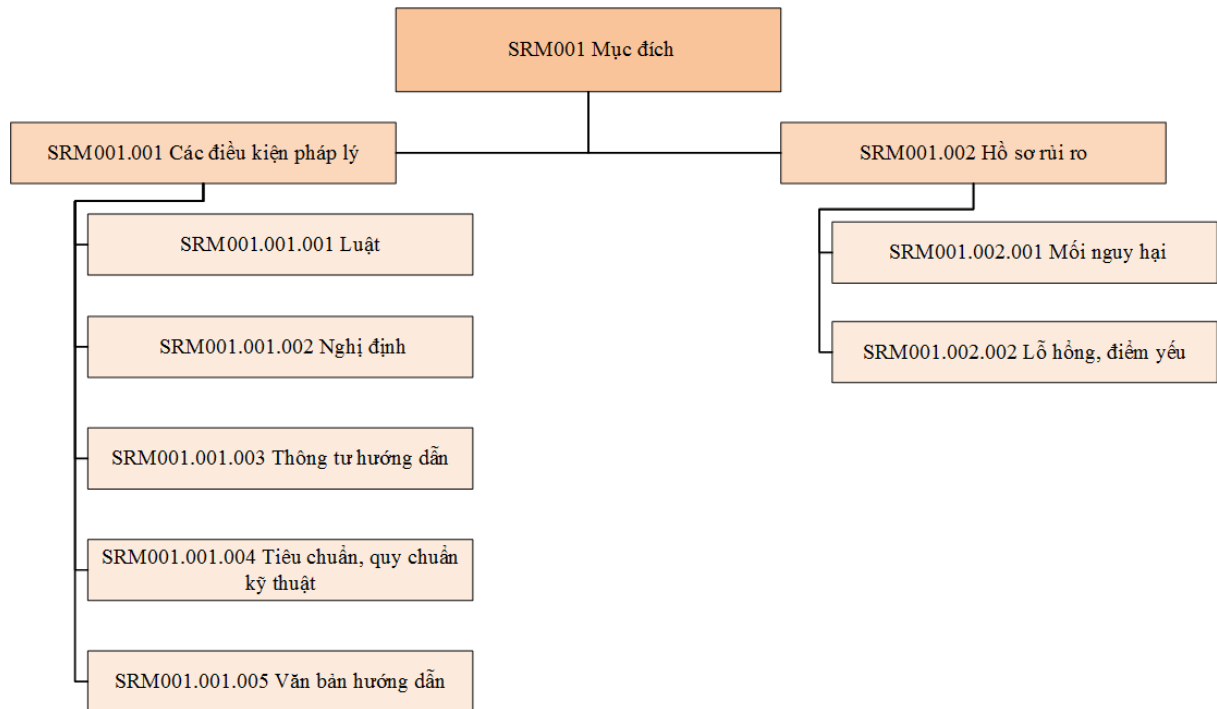
Hình 1: Phân loại mức cao của SRM

| Cấp độ          | Thành phần           | Mô tả   |
|-----------------|----------------------|---|
| <b>Cấp độ 1</b> | SRM001 Mục đích      | Triển khai thực tiễn về bảo mật phải cân bằng giữa việc giảm rủi ro và tuân thủ quy định. Các SRM kết hợp việc tuân thủ các quy định ở cấp độ tổ chức với các vấn đề rủi ro tại cấp độ hệ thống và các ứng dụng để lựa chọn cơ chế bảo mật phù hợp.   |
| <b>Cấp độ 2</b> | SRM002 Rủi ro        | Giảm thiểu rủi ro là lý do cuối cùng cho việc áp dụng kiểm soát bảo mật. Theo NIST SP 800-30, rủi ro là một thước đo cho một thực thể đang bị đe dọa bởi một hoàn cảnh tiềm năng hoặc sự kiện, và thường là một chức năng của: (i) các tác động bất lợi sẽ xảy ra nếu các hoàn cảnh hay sự kiện xảy ra; và (ii) các khả năng xảy ra. Rủi ro được giảm thông qua việc thực hiện kiểm soát tác động tiềm năng hoặc khả năng về một lỗ hổng bị khai thác hoặc thông qua việc loại bỏ các mối đe dọa.   |
| <b>Cấp độ 3</b> | SRM003 Các kiểm soát | Các SRM sử dụng các chính sách từ cấp độ tổ chức để phân loại các giám sát cho một cơ quan hay một ngành cụ thể. SRM cho phép các kiến trúc sư lựa chọn các cơ chế giám sát dựa trên mục đích của một cơ quan cũng như các rủi ro cơ quan có thể gặp phải. Duy trì các giám sát ở cấp độ sẽ có tính kế thừa tại cấp độ hệ thống hoặc ứng dụng, điều này tạo thuận lợi cho việc thiết kế và xác định các yêu cầu của các hệ thống cụ thể. Trong khi cơ chế giám sát FISMA được sử dụng xuyên suốt các cơ quan Chính phủ Liên bang cho phép các cơ quan và nhân viên an ninh kiểm tra, giám sát một hệ thống, SRM sử dụng các giám sát (được lựa chọn bởi các cơ quan hoặc ngành) để xác định, xử lý vấn đề bảo mật trong một hệ thống hoặc ứng dụng. |

### 1.3. SRM001 Mục đích

SRM001 Mục đích Mục đích mô tả các rủi ro đối với tác động kinh doanh và môi trường pháp lý tạo nên các nguyên nhân và trách nhiệm đối với một chương trình

an toàn thông tin mạng.



Hình 2: Cấu trúc phân cấp SRM001 Mục đích

Phân loại chi tiết của Mục đích và Tiêu chuẩn dịch vụ hạ tầng kỹ thuật, công nghệ liên quan được liệt kê trong bảng dưới đây:

| Miền An toàn thông tin mạng | Sự xem xét                       | Ngữ cảnh                                      |
|-----------------------------|----------------------------------|---|
| SRM001 Mục đích             | SRM001.001 Các điều kiện pháp lý | SRM001.001.001 Luật                           |
|                             |                                  | SRM001.001.002 Nghị định                      |
|                             |                                  | SRM001.001.003 Thông tư hướng dẫn             |
|                             |                                  | SRM001.001.004 Tiêu chuẩn, quy chuẩn kỹ thuật |
|                             |                                  | SRM001.001.005 Văn bản hướng dẫn              |
|                             | SRM001.002 Hồ sơ rủi ro          | SRM001.002.001 Mối nguy hại                   |
|                             |                                  | SRM001.002.002 Lỗ hổng, điểm yếu              |

### 1.3.1. SRM001.001 Các điều kiện pháp lý

SRM001.001 Mục đích mô tả các rủi ro làm ảnh hưởng đến hoạt động liên tục của nghiệp vụ và môi trường pháp lý từ đó giúp hình thành nhiệm vụ trong đó xác định rõ phạm vi, mục tiêu, hoạt động, tổ chức thực hiện được hiệu quả.

SRM001.001 Mục đích sẽ đóng vai trò là một tiêu chuẩn chung được áp dụng trong tất cả các cơ quan Chính phủ, để đảm bảo an toàn thông tin mạng của tất cả các ứng dụng của Chính phủ Việt Nam.

Các thành phần thuộc SRM001.001 Mục đích cấp được liệt kê trong bảng dưới đây:

| STT | Ngữ cảnh                                      | Mô tả  |
|-----|---|--|
| 1   | SRM001.001.001 Luật                           | <p>Đề cập đến tất cả các luật về an toàn thông tin mạng áp dụng trong các cơ quan Chính phủ Việt Nam.</p> <p>Các Luật hiện hành:</p> <ul style="list-style-type: none"> <li>- Luật An toàn thông tin mạng năm 2015;</li> <li>- Luật An ninh mạng năm 2018</li> </ul>   |
| 2   | SRM001.001.002 Nghị định                      | <p>Đề cập các nghị định hướng dẫn các luật về an toàn thông tin mạng được áp dụng trong các cơ quan Chính phủ Việt Nam.</p> <p>Các Nghị định hiện hành bao gồm:</p> <ul style="list-style-type: none"> <li>- 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</li> </ul>  |
| 3   | SRM001.001.003 Thông tư hướng dẫn             | <p>Đề cập các nghị định hướng dẫn các luật về an toàn thông tin mạng được áp dụng trong các cơ quan Chính phủ Việt Nam.</p> <p>Các Thông tư hiện hành bao gồm:</p> <ul style="list-style-type: none"> <li>- 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 của Chính phủ về đảm bảo an toàn thông tin hệ thống theo cấp độ</li> </ul> |
| 4   | SRM001.001.004 Tiêu chuẩn, quy chuẩn kỹ thuật | <p>Đề cập các nghị định hướng dẫn các luật về an toàn thông tin mạng được áp dụng trong các cơ quan Chính phủ Việt Nam.</p> <p>Các tiêu chuẩn, quy chuẩn kỹ thuật hiện hành bao gồm:</p> <ul style="list-style-type: none"> <li>(1) TCVN ISO/IEC 27001:2009 Công nghệ thông tin - Hệ thống quản lý an toàn thông tin</li> </ul>  |

|  |  |   |
|--|--|---|
|  |  | <p>tin – Các yêu cầu</p> <p>(2) TCVN ISO/IEC 27002:2011 Công nghệ thông tin-Các kỹ thuật an toàn- Quy tắc thực hành Quản lý an toàn thông tin</p> <p>(3) 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</p> <p>(4) 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</p> <p>(5) 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</p> <p>(6) TCVN 10295:2014 ISO/IEC 27005:2011 Công nghệ thông tin-Các kỹ thuật an toàn-Quản lý rủi ro an toàn thông tin</p> <p>(7) 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</p> <p>(8) 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</p> <p>(9) 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</p> <p>(10) 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</p> |
|--|--|---|

|   |                                  |  |
|---|----------------------------------|--|
|   |                                  | <p>(11) 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</p> <p>(12) TCVN 11239:2015 Công nghệ thông tin - Các kỹ thuật an toàn - Quản lý sự cố an toàn thông tin</p> <p>(13) TCVN 11386:2016 Công nghệ thông tin - Các kỹ thuật an toàn - Phương pháp đánh giá an toàn công nghệ thông tin</p> <p>(14) 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</p> <p>(15) 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</p> <p>(16) 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</p> <p>(17) 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</p> |
| 5 | SRM001.001.005 Văn bản hướng dẫn | <p>Đề cập các nghị định hướng dẫn các luật về an toàn thông tin mạng được áp dụng trong các cơ quan Chính phủ Việt Nam.</p> <p>Các văn bản hướng dẫn hiện hành bao gồm:</p> <ul style="list-style-type: none"> <li>- Văn bản số 2290/BTTTT-CATTTT ngày 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.</li> </ul>  |

### 1.3.2. SRM001.002 Hồ sơ rủi ro

SRM001.002 Hồ sơ rủi ro mô tả về các rủi ro, trong đó, rủi ro là xác suất của một lỗ hổng bị con người khai thác. Các loại rủi ro bao gồm: rủi ro chương trình hoặc rủi ro về mua sắm (ví dụ, chi phí, tiến độ, hiệu suất); sự tuân thủ và rủi ro về quy định; rủi ro tài chính; rủi ro pháp lý; hoạt động (ví dụ, nhiệm vụ hoặc nghiệp vụ) rủi ro; rủi ro chính trị; rủi ro dự án; rủi ro về danh tiếng; rủi ro an toàn; rủi ro hoạch định chiến lược.

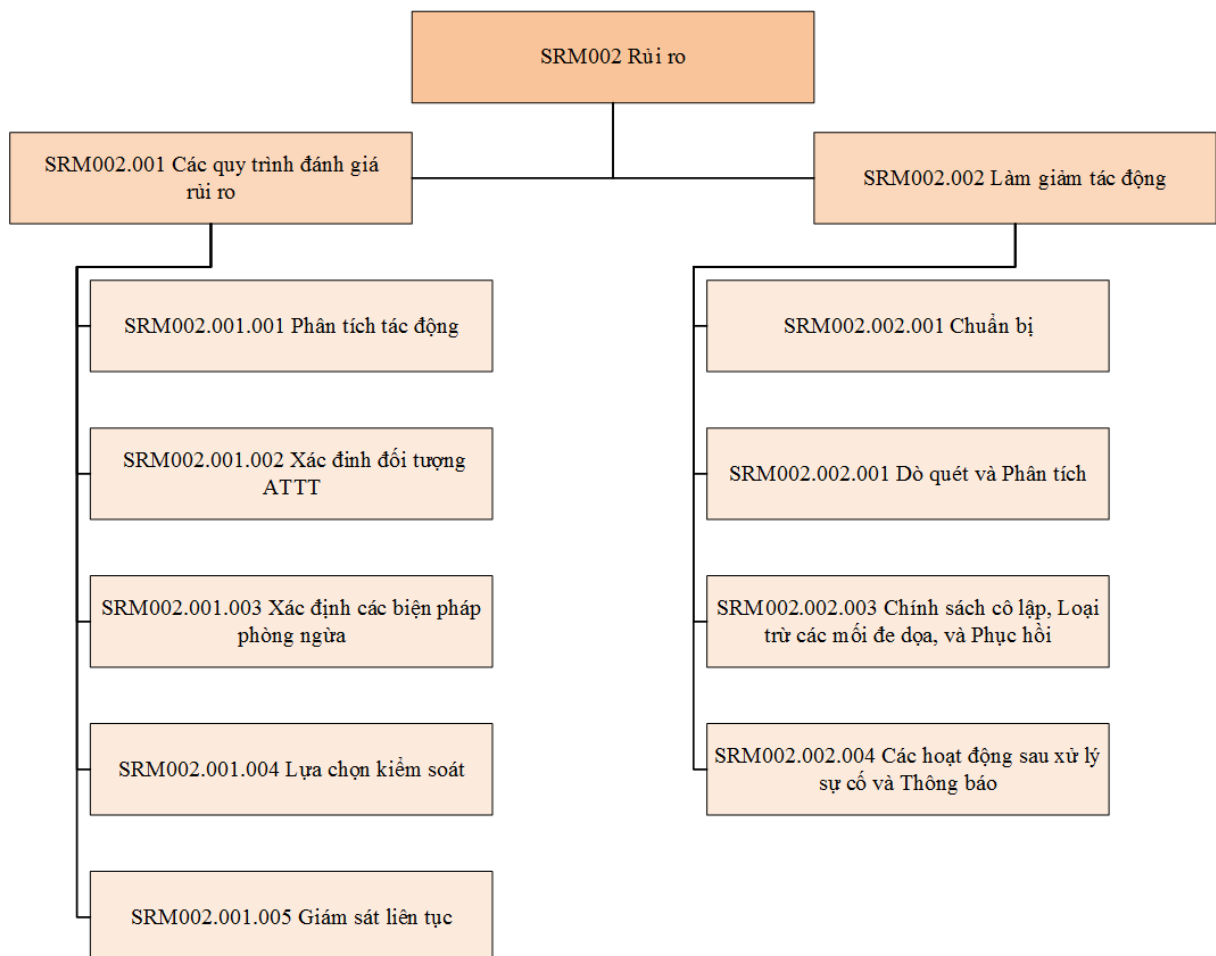


Mô tả về các thành phần thuộc SRM001.002 Hồ sơ rủi ro được liệt kê trong bảng dưới đây:

| STT | Ngữ cảnh                         | Mô tả   |
|-----|----------------------------------|---|
| 1   | SRM001.002.001 Mỗi nguy hại      | Đề cập đến về một mối đe dọa tiềm năng đến các nguồn tài nguyên (vô tình kích hoạt hoặc cố ý khai thác) tạo ra một lỗ hổng cụ thể.  |
| 2   | SRM001.002.002 Lỗ hổng, điểm yếu | Một lỗ hổng hoặc điểm yếu trong quy trình bảo mật hệ thống, thiết kế, thực hiện, hoặc kiểm soát nội bộ có thể bị tấn công (vô tình kích hoạt hoặc cố ý khai thác) và kết quả là một vi phạm an toàn thông tin hoặc vi phạm chính sách bảo mật của hệ thống. |

#### 1.4. SRM002 Rủi ro

SRM002 Rủi ro mô tả các hoạt động như xác định, giảm thiểu và kiểm soát mỗi nguy hại trong một cơ quan, tổ chức.



Hình 3: Cấu trúc phân cấp SRM002 Rủi ro

Phân cấp chi tiết SRM002 Rủi ro được liệt kê trong bảng dưới đây:

| Miền An toàn thông tin mạng | Sự xem xét                               | Ngữ cảnh   |
|-----------------------------|--|--|
| SRM002 Rủi ro               | SRM002.001 Các quy trình đánh giá rủi ro | SRM002.001.001 Phân tích tác động                                      |
|                             |  | SRM002.001.002 Xác định đối tượng ATTT                                 |
|                             |  | SRM002.001.003 Xác định các biện pháp phòng ngừa                       |
|                             |  | SRM002.001.004 Lựa chọn kiểm soát                                      |
|                             |  | SRM002.001.005 Giám sát liên tục                                       |
|                             | SRM002.002 Làm giảm tác động             | SRM002.002.001 Chuẩn bị  |
|                             |  | SRM002.002.001 Dò quét và Phân tích                                    |
|                             |  | SRM002.002.003 Chính sách cô lập, Loại trừ các mối đe dọa, và Phục hồi |
|                             |  | SRM002.002.004 Các hoạt động sau xử lý sự cố và Thông báo              |

#### 1.4.1. SRM002.001 Các quy trình đánh giá rủi ro

SRM002.001 Các quy trình đánh giá rủi ro được sử dụng để xác định các rủi ro đối với các nghiệp vụ của Chính phủ trong ngữ cảnh của một chương trình hay hệ thống CNTT, mức độ rủi ro chấp nhận được, các kiểm soát tương ứng nhằm làm giảm tác động của rủi ro xuống mức chấp nhận thông qua các biện pháp phòng ngừa phù hợp.

Các ngữ cảnh thuộc SRM002.001 Nền tảng phát triển ứng dụng, dịch vụ được liệt kê trong bảng dưới đây:

| STT | Ngữ cảnh                          | Mô tả  |
|-----|-----------------------------------|--|
| 1   | SRM002.001.001 Phân tích tác động | Quá trình xác định các tác động tiềm tàng có thể gây nguy hại cho các thông tin và hệ thống thông tin cần thiết của cơ quan, tổ chức để hoàn thành nhiệm vụ được giao, bảo vệ tài sản của mình, thực hiện đầy đủ trách nhiệm pháp lý của mình, thực hiện các chức năng, nhiệm vụ của mình hàng ngày, |

|   |  |   |
|---|--|---|
|   |  | và bảo vệ cá nhân thuộc cơ quan, tổ chức. Danh mục bảo đảm an toàn thông tin mạng được sử dụng kết hợp với lỗ hổng, điểm yếu và mối nguy hại về lộ lọt thông tin trong việc đánh giá rủi ro đối với một cơ quan, tổ chức.   |
| 2 | SRM002.001.002 Xác định đối tượng ATTT           | Việc này bao gồm tất cả các chức năng liên quan đến việc bảo vệ thông tin và hệ thống thông tin trong các cơ quan Chính phủ tránh khỏi việc truy cập trái phép, sử dụng, lộ lọt, gián đoạn, biến đổi, hoặc hủy hoại.  |
| 3 | SRM002.001.003 Xác định các biện pháp phòng ngừa | Các biện pháp phòng chống theo quy định để đáp ứng các yêu cầu bảo mật (ví dụ đảm bảo tính bảo mật, toàn vẹn và sẵn sàng) quy định đối với một hệ thống thông tin. Biện pháp phòng chống có thể bao gồm các tính năng bảo mật, ràng buộc về quản lý, cán bộ chuyên trách về an toàn thông tin mạng, bảo mật mức vật lý của hệ thống tòa nhà, khu vực, các thiết bị. |
| 4 | SRM002.001.004 Lựa chọn kiểm soát                | Các biện pháp bảo đảm an toàn thông tin mạng tối thiểu, theo đó các biện pháp bảo vệ, kỹ thuật, các thủ tục phải được áp dụng cho các hệ thống thông tin và mạng lưới dựa trên rủi ro, mối nguy hại, lỗ hổng, vấn đề trong kết nối liên thông hệ thống, nhu cầu đảm bảo thông tin.  |
| 5 | SRM002.001.005 Giám sát liên tục                 | Các hoạt động giám sát cần thiết nhằm xác định hiệu quả các kiểm soát an toàn thông tin mạng cũng như việc tuân thủ các quy định, hướng dẫn về bảo đảm an toàn thông tin mạng (Luật, Nghị định, Thông tư, quy chuẩn, tiêu chuẩn kỹ thuật, văn bản hướng dẫn)  |

#### 1.4.2. SRM002.002 Làm giảm tác động

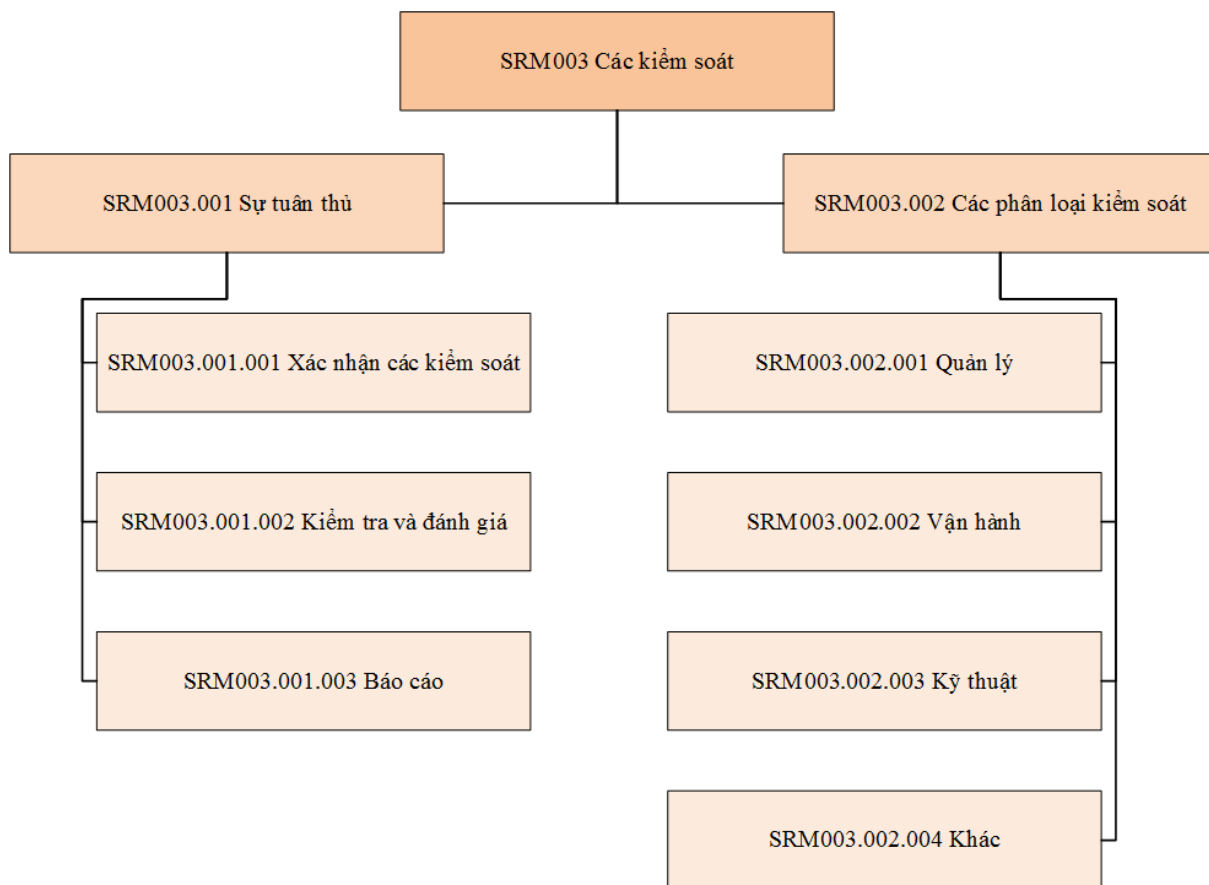
SRM002.002 Làm giảm tác động xem xét các hoạt động cần thiết để giảm thiểu tác động đến cơ quan, tổ chức khi lỗ hổng, điểm yếu được khai thác.

Các nội dung thuộc SRM002.002 Làm giảm tác động được liệt kê trong bảng dưới đây:

| STT | Ngữ cảnh   | Mô tả   |
|-----|--|---|
| 1   | SRM002.002.001 Chuẩn bị  | Các biện pháp chuẩn bị để đảm bảo rằng một cơ quan, tổ chức có thể ứng phó một cách hiệu quả với các sự cố mất an toàn thông tin mạng.  |
| 2   | SRM002.002.001 Dò quét và Phân tích                                    | Các khả năng cần thiết để phát hiện, xác định, đánh giá tác động và xác định trình tự ưu tiên ứng cứu sự cố mất an toàn thông tin mạng.   |
| 3   | SRM002.002.003 Chính sách cô lập, Loại trừ các mối đe dọa, và Phục hồi | Các hoạt động cần thiết để cô lập, loại trừ và phục hồi từ một sự cố mất an toàn thông tin mạng, bao gồm cả tài liệu chứng minh, giảm thiểu việc lỗ hổng, điểm yếu bị khai thác, loại bỏ các lỗ hổng, xác nhận các chức năng hoạt động bình thường trở lại. |
| 4   | SRM002.002.004 Các hoạt động sau xử lý sự cố và Thông báo              | Quá trình thực hiện đánh giá nghiêm túc, rút kinh nghiệm sau sự cố, xác định những thay đổi cần thiết để chính sách an toàn thông tin, cung cấp báo cáo đầy đủ của tất cả các sự cố cho các bên liên quan.  |

### 1.5. SRM003 Các kiểm soát

SRM003 Các kiểm soát là các cơ chế nhằm giảm nhẹ nguy cơ và các tác động của các lỗ hổng, của các sự cố làm mất an toàn thông tin mạng, các mối nguy hại và bao gồm cả việc đánh giá hiệu quả của chúng.



Hình 4: Cấu trúc phân cấp SRM003 Các kiểm soát

Các kiểm soát thuộc SRM003 được liệt kê trong bảng dưới đây:

| Miền An toàn thông tin mạng | Sự xem xét                         | Ngữ cảnh                              |
|-----------------------------|------------------------------------|---------------------------------------|
| SRM003 Các kiểm soát        | SRM003.001 Sự tuân thủ             | SRM003.001.001 Xác nhận các kiểm soát |
|                             |                                    | SRM003.001.002 Kiểm tra và đánh giá   |
|                             |                                    | SRM003.001.003 Báo cáo                |
|                             | SRM003.002 Các phân loại kiểm soát | SRM003.002.001 Quản lý                |
|                             |                                    | SRM003.002.002 Vận hành               |
|                             |                                    | SRM003.002.003 Kỹ thuật               |
|                             |                                    | SRM003.002.004 Khác                   |

### 1.5.1. SRM003.001 Sự tuân thủ

SRM003.001 Sự tuân thủ coi các hoạt động cần thiết để xác nhận và báo cáo về sự hiệu quả của kiểm soát được triển khai áp dụng

Các nội dung thuộc SRM003.001 Sự tuân thủ được liệt kê trong bảng dưới đây:

| STT | Ngữ cảnh                              | Mô tả   |
|-----|---------------------------------------|---|
| 1   | SRM003.001.001 Xác nhận các kiểm soát | Các hoạt động hỗ trợ việc xác nhận các cơ chế kiểm soát.  |
| 2   | SRM003.001.002 Kiểm tra và đánh giá   | Các hoạt động hỗ trợ việc kiểm tra và đánh giá các khả năng và yêu cầu an toàn thông tin mạng.  |
| 3   | SRM003.001.003 Báo cáo                | Các hoạt động cần thiết phải tuân thủ đối với các yêu cầu báo cáo về an toàn thông tin mạng và tính riêng tư, chỉ số về hiệu suất, chi phí liên quan và các thông tin khác. |

### 1.5.2. SRM003.002 Các phân loại kiểm soát

SRM003.002 Các phân loại 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.

Các nội dung thuộc SRM003.003 Các phân loại kiểm soát được liệt kê trong bảng dưới đây:

| STT | Ngữ cảnh                | Mô tả   |
|-----|-------------------------|---|
| 1   | SRM003.002.001 Quản lý  | Các kiểm soát an toàn thông tin mạng (như: biện pháp bảo vệ hoặc biện pháp đối phó) cho một hệ thống thông tin trong đó tập trung vào việc quản lý rủi ro và quản lý an toàn thông tin của hệ thống thông tin.  |
| 2   | SRM003.002.002 Vận hành | Các kiểm soát an toàn thông tin (như: biện pháp bảo vệ hoặc biện pháp đối phó) cho một hệ thống thông tin được thực hiện chủ yếu bởi con người, thay vì thực hiện bởi hệ thống.   |
| 3   | SRM003.002.003 Kỹ thuật | Các kiểm soát an ninh (như: biện pháp bảo vệ hoặc biện pháp đối phó) cho một hệ thống thông tin được thực hiện chủ yếu bởi các hệ thống thông tin thông qua các cơ chế có trong các thành phần phần cứng, phần mềm hoặc firmware (Tường lửa, IDS, IPS, Antivirus, Xác thực người dùng và quản lý quyền truy cập, Mã hóa...) của hệ thống. |

|   |                     |  |
|---|---------------------|--|
| 4 | SRM003.002.004 Khác | Các kiểm soát an toàn thông tin bắt buộc không nằm trong các quy định, hướng dẫn mà nằm ở các văn bản khác như Chỉ thị Thủ tướng, Chỉ thị của Bộ trưởng/Chủ tịch UBND, Các biên bản ghi nhớ... |
|---|---------------------|--|

Cụ thể về các kiểm soát và việc áp dụng các kiểm soát phù hợp được quy định tại:

- 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 của Chính phủ về đảm bảo an toàn thông tin hệ thống theo cấp độ;
- TCVN số 11930:2017/BTTTT Công nghệ thông tin - Các kỹ thuật an toàn - Yêu cầu cơ bản về an toàn thông tin theo cấp độ.