

**Phụ lục XI**  
**Quy trình quản lý rủi ro an toàn thông tin**  
(Kèm theo Quyết định số /QĐ-BNV ngày / /2024  
của Bộ trưởng Bộ Nội vụ)

**Bước 1: Thiết lập bối cảnh**

**- Thông tin tổng quan về hệ thống thông tin**

Bước này cần đưa ra thông tin tổng quan, mục tiêu, quy mô, phạm vi và các thành phần của hệ thống cần bảo vệ, bao gồm nhưng không giới hạn các thông tin sau:

1. Thông tin Chủ quản hệ thống thông tin
2. Thông tin Đơn vị vận hành
3. Chức năng, nhiệm vụ, cơ cấu tổ chức của đơn vị vận hành
4. Các cơ quan, tổ chức liên quan
5. Phạm vi, quy mô của hệ thống.

**- Tiêu chí chấp nhận rủi ro**

Việc xử lý toàn bộ rủi ro được xác định là khó khả thi với bất kỳ cơ quan, tổ chức nào. Do đó, các rủi ro có thể xem xét giảm thiểu đến mức chấp nhận được.

Tiêu chí chấp nhận rủi ro phụ thuộc vào các chính sách, mục đích, mục tiêu bảo đảm an toàn thông tin của cơ quan, tổ chức và các lợi ích của các bên liên quan.

Mỗi tổ chức cần phải xác định mức chấp nhận rủi ro của riêng tổ chức mình. Việc xác định các tiêu chí chấp nhận rủi ro cần xem xét đến các yếu tố như: Nguồn lực để xử lý rủi ro so với hiệu quả mang lại sau khi rủi ro được xử lý; Khả năng xử lý rủi ro theo điều kiện thực tế của cơ quan, tổ chức.

Tiêu chí chấp nhận rủi ro có thể bao gồm nhiều ngưỡng với các tiêu chí tương ứng, căn cứ theo mục tiêu bảo đảm an toàn thông tin mà tổ chức đưa ra một số tiêu chí chấp nhận rủi ro như sau:

1. Hệ thống thông tin cấp độ cấp độ 5 không chấp nhận tồn tại rủi ro.
2. Hệ thống thông tin cấp độ 3 hoặc cấp độ 4, chỉ chấp nhận tồn tại các rủi ro ở mức thấp.
3. Hệ thống thông tin cấp độ 1 hoặc cấp độ 2, không chấp nhận tồn tại các rủi ro mức trung bình.

**- Phạm vi và giới hạn**

Cần xác định rõ phạm vi thực hiện đánh giá và quản lý rủi ro để bảo toàn bộ tài sản được bảo vệ trong quy trình thực hiện. Để xác định phạm vi, giới hạn, cơ quan, tổ chức cần xác định rõ thông tin liên quan (bao gồm nhưng không giới hạn) sau:

1. Phạm vi quản lý an toàn thông tin
  - a) Các mục tiêu bảo đảm an toàn thông tin của cơ quan, tổ chức
  - b) Các quy định pháp lý phải tuân thủ
  - c) Quy chế, chính sách bảo đảm an toàn thông tin của tổ chức.
2. Phạm vi kỹ thuật

a) Sơ đồ tổng thể (vật lý, logic) và các thành phần trong hệ thống (thiết bị mạng, bảo mật, máy chủ, thiết bị đầu cuối...).

b) Xác định các hệ thống thông tin khác có liên quan hoặc có kết nối đến hoặc có ảnh hưởng quan trọng tới hoạt động bình thường của hệ thống thông tin được đề xuất; trong đó, xác định rõ mức độ ảnh hưởng đến hệ thống thông tin đang được đề xuất cấp độ khi các hệ thống này bị mất an toàn thông tin;

c) Danh mục các nguy cơ tấn công mạng, mất an toàn thông tin đối với hệ thống và các ảnh hưởng.

### ***- Tổ chức thực hiện đánh giá và quản lý rủi ro***

Cần xây dựng phương án, kế hoạch thực hiện đánh giá và quản lý rủi ro an toàn thông tin. Nội dung phương án, kế hoạch, trách nhiệm của các đơn vị, bộ phận liên quan cần đưa vào quy chế bảo đảm an toàn thông tin của cơ quan, tổ chức để thực hiện.

Dưới đây là một số nội dung cần thực hiện (bao gồm nhưng không giới hạn) để tổ chức thực hiện đánh giá và quản lý rủi ro an toàn thông tin:

1. Phương án, kế hoạch thực hiện đánh giá và quản lý rủi ro.
2. Quy trình tổ chức thực hiện đánh giá và quản lý rủi ro.
3. Cơ chế phối hợp với các bên liên quan trong quá trình thực hiện.
4. Phương án, kế hoạch giám sát quy trình đánh giá và quản lý rủi ro.

### **Bước 2: Đánh giá rủi ro**

#### ***- Nhận biết rủi ro***

Nhận biết rủi ro là các bước để xác định ra các rủi ro, hậu quả và mức thiệt hại tương ứng, để xác định được rủi ro, cơ quan, tổ chức cần thực hiện các bước sau:

1. Nhận biết về tài sản để xác định danh mục các tài sản của cơ quan, tổ chức cần bảo vệ bao gồm thông tin, hệ thống thông tin.
2. Nhận biết về môi đe dọa để xác định các môi đe dọa đối với mỗi tài sản.
3. Nhận biết về điểm yếu để xác định các điểm yếu có thể tồn tại đối với mỗi tài sản.

Kết quả của bước nhận biết rủi ro là danh mục các môi đe dọa và điểm yếu đối với các tài sản được xác định.

#### ***- Phân tích rủi ro***

Phân tích rủi ro để xác định ra các mức ảnh hưởng, các hậu quả đối với cơ quan, tổ chức trên cơ sở thực hiện bước nhận biết rủi ro ở trên, để phân tích rủi ro, cơ quan, tổ chức cần thực hiện các bước sau:

1. Đánh giá các hậu quả để xác định mức ảnh hưởng đối với cơ quan, tổ chức khi tài sản bị khai thác điểm yếu gây ra các mối nguy.
2. Đánh giá khả năng xảy ra đối với từng loại sự cố.

Kết quả của bước phân tích rủi ro là xác định được các hậu quả, mức ảnh hưởng mà cơ quan, tổ chức phải xử lý.

#### ***- Ước lượng rủi ro***

Ước lượng rủi ro để xác định ra các rủi ro và mức rủi ro tương ứng mà cơ

quan, tổ chức phải xử lý. Mức rủi ro được xác định dựa vào 02 tham số được xác định ở bước trên là mức ảnh hưởng và khả năng xảy ra sự cố.

### **Bước 3: Xử lý rủi ro**

Cơ quan, tổ chức có thể lựa chọn các phương án xử lý rủi ro khác nhau để bảo đảm đạt được các mục tiêu bảo đảm an toàn thông tin của đơn vị mình. Việc thực hiện xử lý rủi ro có thể được thực hiện bởi một hoặc kết hợp nhiều phương án sau: thay đổi rủi ro, duy trì rủi ro, tránh rủi ro và chia sẻ rủi ro, cụ thể như dưới đây.

#### ***- Thay đổi rủi ro***

Thay đổi rủi ro là phương án thực hiện các biện pháp xử lý, khắc phục nhằm giảm mức rủi ro đã được xác định nhằm xác định các rủi ro tồn đọng được đánh giá lại ở mức chấp nhận được.

Để thực hiện phương án này, cơ quan, tổ chức cần xây dựng một hệ thống các biện pháp kiểm soát phù hợp. Các biện pháp được lựa chọn căn cứ vào các tiêu chí liên quan đến chi phí, đầu tư và thời gian triển khai, trên cơ sở cân đối giữa nguồn lực bỏ ra và lợi ích đem lại đối với tổ chức khi thực hiện xử lý rủi ro đó.

#### ***- Duy trì rủi ro***

Duy trì rủi ro là phương án chấp nhận rủi ro đã xác định mà không đưa ra các phương án xử lý để giảm thiểu rủi ro. Việc xác định rủi ro nào có thể được chấp nhận dựa vào mức rủi ro và tiêu chí chấp nhận rủi ro.

#### ***- Tránh rủi ro***

Tránh rủi ro là phương án xử lý khi cơ quan, tổ chức phải đối mặt với mức rủi ro quá cao bằng cách làm thay đổi, loại bỏ hoặc dừng hoạt động của hệ thống, quy trình nghiệp vụ hoặc hoạt động của cơ quan, tổ chức để không phải đối mặt với rủi ro đã xác định. Tránh rủi ro là phương án thích hợp khi rủi ro được xác định vượt quá khả năng chấp nhận rủi ro của tổ chức.

#### ***- Chia sẻ rủi ro***

Chia sẻ rủi ro là phương án chuyển rủi ro, một phần rủi ro phải đối mặt cho cơ quan, tổ chức khác. Phương án chia sẻ rủi ro thường được thực hiện khi cơ quan, tổ chức xác định rằng việc giải quyết rủi ro yêu cầu chuyên môn hoặc nguồn lực được cung cấp tốt hơn bởi các tổ chức khác.

### **Bước 4: Chấp nhận rủi ro**

Chấp nhận rủi ro là việc xem xét, đánh giá các rủi ro tồn đọng, chưa được xử lý hoàn toàn để đánh giá lại mức rủi ro sau xử lý có thể được chấp nhận hay không.

Rủi ro tồn đọng được chấp nhận khi mức rủi ro được xác định là thấp hơn mức rủi ro mà cơ quan, tổ chức có thể chấp nhận dựa vào tiêu chí chấp nhận rủi ro.

### **Bước 5: Truyền thông và tư vấn rủi ro an toàn thông tin**

Truyền thông và tư vấn rủi ro an toàn thông tin là hoạt động nhằm tuyên truyền nâng cao nhận thức cho các bên liên quan đến hoạt động đánh giá và quản lý rủi ro. Bên cạnh đó, việc này cũng nhằm đạt được sự thống nhất giữa các bên

liên quan. Ví dụ trong trường hợp lựa chọn phương án chia sẻ rủi ro.

Cơ quan, tổ chức cần xây dựng kế hoạch truyền thông rủi ro định kỳ hoặc đột xuất. Hoạt động truyền thông rủi ro phải được thực hiện liên tục và thường xuyên.

#### **Bước 6: Giám sát và soát xét rủi ro an toàn thông tin**

Giám sát và soát xét rủi ro nhằm bảo đảm hoạt động đánh giá và quản lý rủi ro an toàn thông tin được thực hiện thường xuyên liên tục theo quy chế, chính sách bảo đảm an toàn thông tin của cơ quan, tổ chức.

##### ***- Giám sát và soát xét các yếu tố rủi ro***

Các rủi ro là không ổn định, các mối đe dọa, những điểm yếu, khả năng xảy ra hoặc những hậu quả có thể thay đổi mà không có bất kỳ dấu hiệu nào. Do đó, việc kiểm tra liên tục là cần thiết để phát hiện những thay đổi này.

Việc giám sát và soát xét các yếu tố rủi ro cần bảo đảm các yếu tố sau:

1. Quản lý được các tài sản mới, sự thay đổi của tài sản, giá trị của tài sản.
2. Sự thay đổi, xuất hiện mới các mối đe dọa
3. Sự thay đổi, xuất hiện mới các điểm yếu
4. Sự thay đổi, xuất hiện mới các rủi ro.

Kết quả của việc giám sát và soát xét các yếu tố rủi ro là việc cập nhật thường xuyên, liên tục sự thay đổi đối với các yếu tố rủi ro được đề cập ở trên.

##### ***- Giám sát soát xét và cải tiến quản lý rủi ro***

Để bảo đảm hoạt động đánh giá và quản lý rủi ro an toàn thông tin được mang lại hiệu quả, việc giám sát, soát xét và cải tiến quy trình quản lý rủi ro an toàn thông tin cần được thực hiện thường xuyên, liên tục.

Các tiêu chí được sử dụng để giám sát soát xét và cải tiến quản lý rủi ro có thể bao gồm, nhưng không giới hạn các yếu tố sau: Các yếu tố liên quan đến quy định pháp lý, Phương pháp tiếp cận đánh giá rủi ro, Các loại tài sản và giá trị tài sản, Tiêu chí tác động, Tiêu chí ước lượng rủi ro, Tiêu chí chấp nhận rủi ro; Các nguồn lực cần thiết...