

# ỨNG DỤNG LÝ THUYẾT QUẢN TRỊ RỦI RO - GIẢI PHÁP BẢO ĐẢM AN TOÀN CHỖ HỆ THỐNG VĂN BẢN ĐIỆN TỬ CỦA CÁC CƠ QUAN, TỔ CHỨC

TRẦN THANH TÙNG\*

*Trong hoạt động của các cơ quan, tổ chức, văn bản điện tử đã và đang trở thành công cụ, phương tiện không thể thiếu để ghi, nhận, trao đổi thông tin. Tuy nhiên, những yếu tố rủi ro đến từ đặc điểm vật mang tin và kỹ năng sử dụng thiết bị điện tử của đội ngũ cán bộ, công chức đã và đang thách thức tính an toàn hệ thống văn bản điện tử hiện nay. Quản trị rủi ro được coi là một giải pháp khoa học nhằm chủ động dự phòng, ứng phó ngăn ngừa, hạn chế khả năng xảy ra rủi ro và giảm thiểu tổn thất. Bài viết phân tích vai trò của quản trị rủi ro, xác định những nội dung cần thực hiện để bảo đảm an toàn đối với văn bản điện tử, từ đó, nâng cao nhận thức, ý thức về quản trị rủi ro đối với cán bộ, công chức, viên chức trong quá trình sử dụng văn bản điện tử.*

*Từ khóa:* Quản trị rủi ro; văn bản điện tử; cơ quan, tổ chức; bảo đảm an toàn.

*Electronic documents have become an indispensable tool and means for recording, receiving and exchanging information in operation of agencies and organizations. However, the risks arising from the information carriers and public officers' use of electronic devices have been challenging the safety of the current electronic document system. Risk management is considered a scientific solution to proactively prevent, respond, prevent, mitigate the possibility of risks and reduce losses. The paper analyzed the role of risk management, identified what to do to ensure safety of electronic documents, thereby raising public officer's awareness of risk management in using electronic documents.*

*Keywords:* Risk management; electronic documents; agencies and organizations; ensure safety.

NGÀY NHẬN: 26/02/2022

NGÀY PHẢN BIỆN, ĐÁNH GIÁ: 22/3/2022

NGÀY DUYỆT: 15/4/2022

## 1. Khái niệm và đặc điểm của văn bản điện tử

Cùng với sự phát triển của khoa học - kỹ thuật, văn bản hình thành trong hoạt động của các cơ quan, tổ chức không chỉ tồn tại dưới dạng bản in truyền thống mà một loại hình văn bản mới được ra đời và ngày càng trở nên phổ biến - đó là văn bản điện tử (VBĐT).

Với những tiện ích vượt trội về khả năng lưu trữ, tốc độ truyền, khai thác thông tin hiệu quả, không bị giới hạn bởi không gian, thời gian, xu hướng VBĐT dần thay thế văn bản giấy ngày càng hiện hữu và trở thành xu thế không thể đảo ngược.

\* TS, Trường Đại học Khoa học Xã hội và Nhân văn, Đại học Quốc gia Hà Nội

Thuật ngữ và khái niệm VBĐT chính thức được đề cập lần đầu tiên tại Nghị định số 64/2007/NĐ-CP ngày 10/4/2007 của Chính phủ về ứng dụng công nghệ thông tin trong hoạt động của cơ quan nhà nước. Theo đó VBĐT được hiểu là văn bản thể hiện dưới dạng thông điệp dữ liệu. Tại Quyết định số 28/QĐ-TTg ngày 12/7/2018 của Thủ tướng Chính phủ về việc gửi, nhận VBĐT giữa các cơ quan trong hệ thống hành chính, khái niệm VBĐT có sự thay đổi với việc xác định phương thức tạo lập và yêu cầu thể thức định dạng. Quan niệm thống nhất về VBĐT một lần nữa được khẳng định tại Nghị định số 30/2020/NĐ-CP ngày 05/3/2020 của Chính phủ về công tác văn thư với nội dung VBĐT là văn bản dưới dạng thông điệp dữ liệu được tạo lập hoặc được số hóa từ văn bản giấy và trình bày đúng thể thức, kỹ thuật, định dạng theo quy định.

Từ đặc tính của thông điệp dữ liệu là thông tin được tạo ra, được gửi đi, được nhận và được lưu trữ bằng phương tiện điện tử cho thấy đặc điểm của VBĐT phải gắn liền với thiết bị điện tử. Đối với VBĐT, con người không thể dựa vào các giác quan để nhận biết thông tin. Vì vậy, để sử dụng được văn bản, cơ quan, tổ chức phải đáp ứng các yêu cầu tối thiểu đặt ra là phải có hệ thống máy tính, hệ thống mạng, cùng với đó là các phần mềm chuyên dụng. Thiết bị điện tử không thể tự vận hành nên cần có nhân lực quản lý hệ thống, người sử dụng thiết bị cần có kỹ năng ứng dụng, khai thác các chức năng để nhận biết, sử dụng thông điệp dữ liệu được truyền tải.

Trên thiết bị điện tử, thông tin không bị giới hạn bởi không gian, khoảng cách địa lý, thời gian truyền tin nhanh chóng đến nhiều đối tượng cùng thời điểm, quá trình xử lý có sự kết nối trực tiếp giữa nhiều tổ chức, cá nhân có liên quan... Tuy nhiên, loại hình văn bản này cũng phải đối mặt với nhiều nguy cơ, thách thức trong việc bảo đảm an toàn của hệ thống cơ sở dữ liệu, như: thiết bị điện tử có khả năng bị hacker tấn công chiếm quyền điều khiển từ bên ngoài, bị nhiễm mã độc, hệ

thống cơ sở dữ liệu dễ bị đột nhập đánh cắp..., hay đôi khi chỉ một phút chủ quan, nhầm lẫn, bất cẩn của người sử dụng có thể làm thiết bị nhiễm mã độc, từ đó, cơ sở dữ liệu bị rò rỉ, bị chỉnh sửa hoặc bị mất...

## 2. Sự cần thiết quản trị rủi ro đối với hệ thống văn bản điện tử tại các cơ quan, tổ chức ở Việt Nam

Một là, VBĐT ngày càng trở nên phổ biến và trở thành công cụ, phương tiện truyền tải, lưu trữ thông tin quan trọng không thể thiếu phục vụ cho hoạt động của các cơ quan, tổ chức.

Theo tinh thần Nghị quyết số 30c/NĐ-CP ngày 08/11/2011 của Chính phủ ban hành *Chương trình tổng thể cải cách hành chính nhà nước giai đoạn 2011 - 2020* thì từ năm 2020, 90% các văn bản, tài liệu chính thức trao đổi giữa các cơ quan hành chính nhà nước được thực hiện dưới dạng điện tử. Điều này cho thấy, khối lượng tài liệu, VBĐT hình thành trong hoạt động của các cơ quan, tổ chức ngày càng phổ biến, phong phú về số lượng và nội dung. Đó là hệ thống cơ sở dữ liệu quan trọng, chứa đựng những thông tin minh chứng phản ánh quá trình hoạt động của cơ quan, tổ chức nếu không may xảy ra rủi ro thì những thiệt hại, tổn thất về dữ liệu là không thể đo đếm.

Hai là, thực hiện quản trị rủi ro (QTRR) sẽ giúp các cơ quan, tổ chức xây dựng ý thức dự phòng, giảm thiểu nguy cơ trong quá trình sử dụng VBĐT.

Thực tế cho thấy, VBĐT có mức độ rủi ro cao hơn văn bản giấy. Thông điệp dữ liệu điện tử được tạo lập, truyền tải, lưu trữ, khai thác từ máy tính, trên mạng sẽ có nguy cơ bị đánh cắp, bị phá hủy với số lượng lớn trong một khoảng thời gian ngắn nếu bị nhiễm virus, sâu máy tính hoặc phần mềm gián điệp. Trong môi trường điện tử, những tác nhân gây hại luôn tồn tại và chỉ một thao tác nhầm lẫn hay một hành động sơ suất của con người sẽ gây ra những thiệt hại lớn đối với dữ liệu thông tin.

Hiện nay, các chuyên gia công nghệ thông tin đã có nhiều giải pháp để bảo đảm an toàn,

phòng, chống những nguy cơ, rủi ro đối với thiết bị điện tử và hệ thống dữ liệu thông tin điện tử. Tuy nhiên, mật mã, mật khẩu dù được thiết kế phức tạp đến đâu thì vẫn tồn tại nguy cơ bị phá hoại. Vì vậy, luôn chủ động xây dựng ý thức về rủi ro cho cán bộ là cách tốt nhất để dự phòng, ngăn chặn, ứng phó rủi ro. Ý thức về rủi ro là phản ứng của cán bộ, công chức, viên chức đối với những rủi ro mà họ phải đối mặt. Ý thức về rủi ro được chia thành ba giai đoạn: ý thức trước khi xảy ra rủi ro, ý thức trong khi xảy ra rủi ro và ý thức sau khi xảy ra rủi ro. Xây dựng được ý thức về rủi ro một cách khoa học, khi rủi ro xảy đến, mọi người sẽ ở trong trạng thái chủ động, có sự chuẩn bị trước, tích cực áp dụng các phương pháp đúng đắn để ứng phó với rủi ro.

Ba là, QTRR sẽ là công cụ, phương tiện giúp các cơ quan, tổ chức thiết lập cơ chế cảnh báo sớm về những rủi ro.

Cảnh báo sớm là “gửi cảnh báo trước”, chỉ cảm giác dữ liệu về một sự việc nào đó có khả năng phát sinh. Trên thực tế, cơ chế cảnh báo sớm về rủi ro là một sự chuẩn bị trước khi sự việc phát sinh nhằm phòng tránh và giảm thiểu rủi ro. Khi nguy cơ sắp xảy ra, hệ thống sẽ kịp thời gửi cảnh báo, từ đó, giảm thiểu được sự hao phí thời gian để phán đoán liệu rủi ro có xảy ra hay không, từ đó nâng cao tốc độ phản ứng với nguy cơ. Khoảng thời gian đầu khi rủi ro xảy ra, áp dụng các biện pháp phản ứng nhanh có thể loại bỏ hoặc ngăn chặn được sự khuếch tán của nguy cơ, giảm thiểu được những tổn thất. So sánh với việc ứng phó khẩn cấp và cấp cứu sau khi rủi ro xảy ra, một cơ chế cảnh báo sớm kiện toàn sẽ mang lại hiệu quả rõ rệt đối với việc phòng tránh và giảm thiểu thiệt hại. Việc xây dựng cơ chế cảnh báo sớm về những rủi ro sẽ có ý nghĩa trong việc bố trí và thực hiện tốt các chính sách và biện pháp khi phát sinh rủi ro; tạo ra sự chuẩn bị tốt về mặt tư tưởng, tổ chức, cơ chế, vật tư và kỹ thuật; góp phần xác định rõ các hành vi thao tác cụ thể để ứng phó với các loại rủi ro; tạo ra sự bảo đảm chắc chắn

khi các rủi ro có khả năng phát sinh trong tương lai; đưa các rủi ro vào trạng thái có thể kiểm soát được bảo đảm sự an toàn đối với trang thiết bị và cơ sở dữ liệu.

### 3. Thực hiện các nội dung quản trị rủi ro đối với hệ thống văn bản điện tử

QTRR là hệ thống các biện pháp nhằm chủ động dự phòng ứng phó trước khi những tình huống mang đến thiệt hại tổn thất có thể xảy ra. Theo đó, nội dung QTRR bao gồm:

*Thứ nhất, nhận diện nguy cơ rủi ro.*

Nhận diện rủi ro là quá trình xác định liên tục và có hệ thống các rủi ro trước khi nảy sinh. Hoạt động nhận diện rủi ro nhằm thu thập về đối tượng có thể gặp rủi ro, các nguồn phát sinh rủi ro, các yếu tố mạo hiểm, hiểm họa, các loại tổn thất mà rủi ro có thể gây ra. Thực tế cho thấy, có quá nhiều mối nguy cơ dẫn đến rủi ro bất ngờ và khó lường trong quá trình sử dụng, khai thác cơ sở dữ liệu thông tin trên VBĐT. Vì vậy, chủ động nhận diện rủi ro là một giải pháp giúp cho các cơ quan, tổ chức tiếp cận rủi ro từ nguy cơ, nguồn gốc phát sinh nhằm xây dựng bảo đảm an toàn hệ thống một cách toàn diện và khoa học.

Xuất phát từ đặc điểm của VBĐT, hoạt động nhận diện rủi ro cần thực hiện trên cơ sở kết quả kiểm tra, đánh giá rà soát quy chế, chính sách bảo đảm an toàn thông tin để tìm ra các điểm yếu chưa đáp ứng các biện pháp quản lý theo quy định. Điểm yếu được ghi nhận trong quá trình đánh giá chính là nhược điểm mà từ đó có thể bị khai thác mang lại những thiệt hại tổn thất. Nhận diện đúng, đủ, kịp thời các điểm yếu sẽ là cơ sở để đánh giá mức độ nguy cơ rủi ro, từ đó, xây dựng các biện pháp ứng phó, ngăn ngừa.

*Thứ hai, thực hiện đo lường nguy cơ rủi ro để đánh giá khả năng xảy ra, mức độ thiệt hại.*

Đây là việc quan trọng không thể thiếu nhưng mới chỉ là công việc khởi đầu của QTRR. Sau khi nhận diện rủi ro, bước tiếp theo là phải tiến hành phân tích, đánh giá để đo lường xác định mức độ nguy cơ theo các thang bậc về rủi ro. Giá trị đo lường được xác

định với mức độ cao - thấp trong một khoảng thời gian xác định.

Theo lý thuyết QTRR, có thể áp dụng phương pháp định lượng thực hiện đo lường, đánh giá nguy cơ rủi ro thông qua các thang điểm từ 1- 5, với mức độ từ rất thấp đến rất cao. Thang đánh giá được thiết lập trên giả thuyết “Nếu các điểm yếu, nguy cơ được cơ quan, tổ chức nhận diện đầy đủ, chính xác, có biện pháp kiểm soát thì rủi ro, nguy cơ rủi ro sẽ giảm và ngược lại nếu điểm yếu, nguy cơ rủi ro không được nhận diện, không có biện pháp kiểm soát thì rủi ro và nguy cơ rủi ro thì tăng”. Mỗi điểm yếu, nguy cơ rủi ro được nhận diện đại diện cho một biến quan sát theo giả thuyết được tạo lập. Thông tin đánh giá được khảo sát qua phiếu đánh giá trực tiếp hoặc online. Các đối tượng thực hiện đánh giá là cán bộ quản lý, cán bộ chuyên môn có liên quan trực tiếp tới quản lý, điều hành hệ thống; khai thác, sử dụng VBĐT tại cơ quan, tổ chức. Điểm trung bình chung đánh giá sẽ là cơ sở xác định mức độ nguy cơ xảy ra rủi ro đối với từng điểm yếu. Khả năng xảy ra rủi ro được đo từ mức độ rất thấp đến rất cao; mức độ tác động của rủi ro từ rất thiệt hại tới thiệt hại không đáng kể. Trên cơ sở kết quả đo lường, đánh giá, cơ quan, tổ chức sẽ lựa chọn xác định các biện pháp kỹ thuật, quản lý để kiểm soát, phòng ngừa dựa trên những nguồn lực và điều kiện khả năng nhằm bảo đảm tính khả thi cho các biện pháp được áp dụng.

*Thứ ba, kiểm soát, phòng ngừa.*

Đây được coi là công việc trọng tâm, cốt lõi của QTRR. Trên thực tế, có thể nhận thấy, khi cơ quan, tổ chức chủ động với kiểm soát, đối phó các rủi ro sẽ góp phần hoàn thiện nhiều mục tiêu khác. Các biện pháp kiểm soát, phòng ngừa phải chỉ ra được mọi tình huống khẩn cấp và nguy cơ mà cơ quan có thể gặp phải; đồng thời đưa ra được biện pháp phản ứng tức thời cũng như việc xử lý dài hạn và nỗ lực khôi phục khi cần thiết. Tuy nhiên, để các biện pháp QTRR có tính thực tiễn đòi hỏi cơ quan, tổ chức phải một kế hoạch, quy trình kiểm soát, ứng phó rủi ro hiệu quả.

Kế hoạch cần có 3 đặc tính quan trọng đó là: *tính toàn diện, đơn giản và linh hoạt*. Kế hoạch phải đưa ra được biện pháp phản ứng tức thời cũng như việc xử lý dài hạn, nỗ lực khôi phục khi cần thiết và dễ thực hiện. Tuy nhiên, kế hoạch không thể đi sâu vào mọi chi tiết phải bảo đảm rằng những gì được đề cập bao gồm những hướng dẫn cơ bản nhưng cũng cho phép sáng tạo trên thực tế. Quy trình, kế hoạch ứng phó với rủi ro hoàn hảo đến đâu thì nó cũng trở nên vô ích nếu như các nhân viên không biết về nó. Do vậy, khi kế hoạch, quy trình được xây dựng cần có biện pháp để hướng dẫn cho nhân viên về các bước thực hiện. Mỗi nhân viên cần phải nhận thức được nhiệm vụ của mình trong quy trình, kế hoạch ứng phó rủi ro được xây dựng.

#### 4. Kết luận

VBĐT là loại hình văn bản mới, sản phẩm của xã hội công nghệ thông tin, tính ưu việt đã được khẳng định nhưng những nguy cơ rủi ro ẩn chứa với hệ thống dữ liệu mà phương tiện chứa đựng và truyền tải còn nhiều ẩn số thách thức đối với các nhà khoa học và quản lý. Nghiên cứu nhận diện, đo lường, đánh giá sẽ là cách thức chủ động bảo đảm an toàn hệ thống thông tin dữ liệu trong VBĐT không chỉ có ý nghĩa tới hoạt động của cơ quan, tổ chức ở hiện tại mà còn mang giá trị lịch sử lâu dài □

#### Tài liệu tham khảo:

1. Công văn số 3001/BTTTT-CATTT ngày 06/9/2019 của Bộ Thông tin và Truyền thông về việc hướng dẫn bảo đảm an toàn thông tin cho hệ thống quản lý văn bản.
2. Cục An toàn thông tin. Tài liệu hướng dẫn đánh giá rủi ro an toàn thông tin năm 2021.
3. Nghị định số 30/2020/NĐ-CP ngày 05/3/2020 của Chính phủ về công tác văn thư.
4. Nghị định số 64/2007/NĐ-CP ngày 10/4/2007 của Chính phủ về ứng dụng công nghệ thông tin trong hoạt động của cơ quan nhà nước.
5. Quyết định số 28/QĐ-TTg ngày 12/7/2018 của Thủ tướng Chính phủ về việc gửi, nhận văn bản điện tử giữa các cơ quan trong hệ thống hành chính.
6. Quản trị rủi ro và khủng hoảng. H. NXB Thống kê, 2005.