CÂN BẰNG GIỮA BẢO MẬT VÀ MINH BẠCH THÔNG TIN KẾ TOÁN TÀI CHÍNH TRONG BỐI CẢNH CHUYỂN ĐỔI SỐ TẠI DOANH NGHIỆP VIỆT NAM

● TRẦN THỊ VÂN[1] - TRẦN THỊ THU HÀ[1]
[1]Trường Đại học Hải Phòng
DOI: https://doi.org/10.62831/202602014

TÓM TẮT:

Trong bối cảnh chuyển đổi số đang diễn ra mạnh mẽ trong mọi lĩnh vực kinh tế - xã hội, hoạt động kế toán tài chính cũng đứng trước yêu cầu cấp thiết về việc vừa đảm bảo bảo mật thông tin, vừa nâng cao tính minh bạch nhằm đáp ứng nhu cầu quản trị nội bộ, nhu cầu của nhà đầu tư và cơ quan quản lý nhà nước. Bài viết tập trung phân tích cơ sở lý luận về mối quan hệ giữa bảo mật và minh bạch thông tin kế toán tài chính, đánh giá thực trạng vấn đề tại Việt Nam trong thời kỳ công nghệ số, đồng thời đề xuất một số giải pháp nhằm hướng tới sự hài hòa giữa tính bảo mật và tính minh bạch trong công bố thông tin kế toán tài chính của doanh nghiệp.

Từ khóa: bảo mật thông tin, minh bạch thông tin, kế toán - tài chính, thông tin kế toán tài chính, công nghệ số, doanh nghiệp Việt Nam.

1. Đặt vấn đề

Trong bối cảnh chuyển đổi số diễn ra mạnh mẽ, hoạt động kế toán tài chính đang đứng trước yêu cầu phải vừa đảm bảo tính bảo mật thông tin, vừa tăng cường tính minh bạch để đáp ứng nhu cầu của nhà quản trị, nhà đầu tư và cơ quan quản lý. Sự phát triển của các công nghệ như ERP, điện toán đám mây, trí tuệ nhân tạo hay blockchain giúp doanh nghiệp nâng cao hiệu quả xử lý và công bố thông tin, song cũng tiềm ẩn nhiều rủi ro về an ninh mạng và rò rỉ dữ liệu tài chính. Việc tìm ra điểm cân bằng hợp lý giữa 2 yếu tố này trở thành vấn đề trọng yếu trong công tác kế toán hiện đại.

Tại Việt Nam, cùng với việc thực hiện chuyển đổi số và lộ trình áp dụng Chuẩn mực Báo cáo tài chính quốc tế (IFRS), yêu cầu minh bạch thông tin tài chính ngày càng được đề cao. Tuy nhiên, trong thực tế, nhiều doanh nghiệp vẫn gặp khó khăn trong việc đảm bảo an toàn dữ liệu và tuân thủ quy định pháp lý về bảo mật. Vì vậy, việc nghiên cứu vấn đề cân bằng giữa bảo mật và minh bạch thông tin kế toán tài chính trong thời kỳ công nghệ số là cần thiết, nhằm góp phần hoàn thiện hệ thống thông tin kế toán và nâng cao tính tin cậy, bền vững trong quản trị tài chính doanh nghiệp.

2. Cơ sở lý thuyết về vấn đề cân bằng giữa bảo mật và minh bạch thông tin kế toán tài chính

Trong nền kinh tế tri thức và bối cảnh chuyển đổi số, thông tin kế toán tài chính được xem là một loại tài sản đặc biệt, có vai trò then chốt trong quản trị doanh nghiệp, ra quyết định đầu tư và giám sát hoạt động tài chính. Giá trị của thông tin kế toán không chỉ thể hiện ở nội dung số liệu mà còn ở mức độ tin cậy, khả năng tiếp cận và mức độ an toàn trong suốt quá trình thu thập, xử lý, lưu trữ và công bố. Bảo mật thông tin kế toán tài chính được hiểu là quá trình bảo vệ dữ liệu kế toán trước các nguy cơ truy cập, sử dụng, thay đổi hoặc tiết lộ trái phép. Trong môi trường số hóa, bảo mật thông tin không chỉ giới hạn ở các biện pháp kỹ thuật như mã hóa, sao lưu hay tường lửa, mà còn bao gồm các yếu tố tổ chức, pháp lý và đạo đức nghề nghiệp. Về mặt lý thuyết, bảo mật thông tin kế toán dựa trên 3 nguyên tắc cốt lõi: tính toàn vẹn, tính sẵn sàng và tính bí mật. Tính toàn vẹn đảm bảo dữ liệu không bị sửa đổi sai lệch; tính sẵn sàng đảm bảo thông tin có thể được truy cập kịp thời bởi người có thẩm quyền; và tính bí mật bảo vệ dữ liệu khỏi các đối tượng không được phép. Việc vi phạm bất kỳ nguyên tắc nào đều có thể làm suy giảm độ tin cậy của hệ thống kế toán và ảnh hưởng tiêu cực đến uy tín doanh nghiệp.

Song song với yêu cầu bảo mật, minh bạch thông tin kế toán tài chính là điều kiện cần thiết để đảm bảo sự vận hành lành mạnh của thị trường tài chính. Minh bạch được hiểu là việc cung cấp thông tin tài chính một cách trung thực, rõ ràng, đầy đủ, kịp thời và có thể kiểm chứng. Theo Tổ chức Hợp tác và Phát triển Kinh tế, minh bạch là một trong những trụ cột của quản trị công ty hiện đại, góp phần giảm thiểu gian lận, hạn chế bất cân xứng thông tin và tăng cường trách nhiệm giải trình của doanh nghiệp. Trong kế toán, minh bạch gắn liền với các nguyên tắc cơ bản như trung thực, khách quan, nhất quán và có khả năng so sánh, qua đó giúp người sử dụng thông tin đánh giá đúng tình hình tài chính và hiệu quả hoạt động của doanh nghiệp.

Các lý thuyết nền tảng của kế toán hiện đại cũng gợi mở những cách tiếp cận khác nhau để hiểu rõ hơn mối quan hệ này. Lý thuyết ủy nhiệm cho thấy, minh bạch thông tin giúp giảm thiểu bất cân xứng thông tin giữa chủ sở hữu và nhà quản lý, nhưng đồng thời làm gia tăng yêu cầu bảo mật để tránh rủi ro rò rỉ dữ liệu. Lý thuyết thông tin bất cân xứng nhấn mạnh thiếu minh bạch có thể dẫn đến các quyết định đầu tư sai lệch và rủi ro đạo đức. Bên cạnh đó, lý thuyết các bên liên quan cho thấy, doanh nghiệp có trách nhiệm cung cấp thông tin phù hợp cho nhiều nhóm đối tượng khác nhau, trong khi lý thuyết thể chế nhấn mạnh vai trò của môi trường pháp lý, chuẩn mực kế toán và thông lệ quốc tế trong việc định hình hành vi công bố và bảo vệ thông tin.

Trong bối cảnh công nghệ số, sự phát triển của các hệ thống ERP, điện toán đám mây, trí tuệ nhân tạo và blockchain đã làm thay đổi căn bản cách thức xử lý và công bố thông tin kế toán. Các công nghệ này vừa tạo điều kiện tăng cường tính minh bạch, vừa đặt ra những thách thức mới về bảo mật dữ liệu và quyền riêng tư. Do đó, việc nghiên cứu cơ sở lý thuyết về cân bằng giữa bảo mật và minh bạch thông tin kế toán tài chính có ý nghĩa quan trọng, làm nền tảng cho việc đánh giá thực trạng và đề xuất giải pháp phù hợp trong bối cảnh chuyển đổi số tại Việt Nam.

Như vậy, cơ sở lý thuyết cho thấy, bảo mật và minh bạch không phải là 2 mục tiêu loại trừ lẫn nhau, mà là 2 yếu tố cần được kết hợp hài hòa trong một khuôn khổ quản trị thông tin thống nhất. Việc xây dựng và vận hành hệ thống thông tin kế toán vừa minh bạch, vừa an toàn là nền tảng quan trọng để nâng cao chất lượng báo cáo tài chính, tăng cường niềm tin của thị trường và tạo tiền đề cho sự phát triển bền vững của doanh nghiệp trong bối cảnh chuyển đổi số.

3. Thực trạng vấn đề cân bằng giữa bảo mật và minh bạch thông tin kế toán tài chính tại Việt Nam hiện nay

Quá trình số hóa công tác kế toán tại Việt Nam diễn ra nhanh chóng trong những năm gần đây: nhiều doanh nghiệp, đặc biệt là các công ty niêm yết và doanh nghiệp lớn, đã chuyển sang sử dụng hệ thống ERP, dịch vụ kế toán trên nền tảng đám mây và các công cụ phân tích dữ liệu tự động nhằm nâng cao hiệu quả xử lý, độ chính xác và tốc độ lập báo cáo tài chính. Song song với xu hướng này, Nhà nước cũng đã hoàn thiện hệ khung pháp lý liên quan đến bảo vệ dữ liệu và an ninh mạng nhằm bảo đảm an toàn thông tin trên không gian số; tiêu biểu là Luật An ninh mạng (2018) và Nghị định số 13/2023/NĐ-CP về bảo vệ dữ liệu cá nhân, tạo cơ sở cho trách nhiệm bảo mật của tổ chức, doanh nghiệp và quyền của chủ thể dữ liệu.

Mặc dù khung pháp lý dần được hoàn thiện, nhưng thực tế triển khai tại doanh nghiệp còn nhiều hạn chế. Ở chiều minh bạch, lộ trình áp dụng Chuẩn mực Báo cáo Tài chính Quốc tế (IFRS) và yêu cầu công bố thông tin chặt chẽ hơn khiến doanh nghiệp phải công khai nhiều dữ liệu hơn, từ các chính sách kế toán đến thông tin về rủi ro, giao dịch liên kết và các công cụ tài chính; điều này đặt áp lực tăng cường tính minh bạch nhưng đồng thời làm dấy lên lo ngại về việc bảo vệ các thông tin chiến lược, dữ liệu khách hàng hay thông tin cá nhân nhạy cảm. Lộ trình IFRS cũng đòi hỏi năng lực hạch toán, kiểm toán và quản trị rủi ro thông tin cao hơn ở các doanh nghiệp niêm yết và tập đoàn lớn, tạo ra khó khăn cho doanh nghiệp vừa và nhỏ trong việc cân bằng giữa công bố đầy đủ và bảo vệ bí mật kinh doanh.

Tình trạng năng lực quản trị an toàn thông tin và nhận thức về bảo mật giữa các tầng lớp doanh nghiệp có khoảng cách lớn. Các tập đoàn lớn, ngân hàng và một số doanh nghiệp niêm yết đã đầu tư hệ thống bảo mật, phân quyền truy cập, mã hóa dữ liệu và kiểm tra nội bộ, nhưng phần lớn doanh nghiệp vừa và nhỏ (SME) vẫn chưa trang bị đầy đủ giải pháp kỹ thuật, chính sách nội bộ và nhân lực chuyên trách để bảo vệ dữ liệu kế toán. Điều này xuất phát từ chi phí đầu tư, thiếu chuyên môn an ninh mạng, và ưu tiên ngắn hạn về hiệu quả hoạt động so với chi phí IT. Điều này dẫn tới hậu quả là rủi ro rò rỉ dữ liệu, lừa đảo trực tuyến diễn ra với mức độ đáng kể trong nhiều ngành, đặc biệt là tài chính, thương mại điện tử và dịch vụ công nghệ. Các báo cáo chuyên môn cho thấy, số lượng sự cố tấn công mạng vẫn cao, điều này nhấn mạnh tính dễ tổn thương của hệ thống thông tin doanh nghiệp khi số hóa nhưng thiếu biện pháp phòng vệ thích hợp.

Một điểm thực tiễn đáng lưu ý là mâu thuẫn giữa nhu cầu minh bạch cho các bên liên quan và nhu cầu bảo mật đối với thông tin nhạy cảm. Trong nhiều trường hợp, các bộ phận quản trị tại doanh nghiệp còn lúng túng khi xác định phạm vi công bố: những thông tin nào bắt buộc phải công khai theo quy định và lợi ích công chúng, và những thông tin nào cần được bảo vệ để duy trì lợi thế cạnh tranh hoặc bảo vệ bí mật khách hàng. Kết quả là một số doanh nghiệp lựa chọn công khai tối thiểu để tránh rủi ro bảo mật, dẫn đến vấn đề thiếu minh bạch, trong khi số khác công bố rộng rãi nhưng chưa thiết lập đầy đủ biện pháp kỹ thuật và thủ tục kiểm soát để bảo vệ dữ liệu công bố khỏi việc bị khai thác sai mục đích. Rào cản này là lý do khiến cơ quan quản lý và nhà đầu tư đôi khi nghi ngờ tính đầy đủ và tin cậy của thông tin tài chính, làm giảm hiệu quả của thị trường vốn nội địa.

Về kiểm soát nội bộ và kiểm toán, thực trạng cho thấy hệ thống kiểm soát nội bộ của nhiều doanh nghiệp chưa bắt kịp với mô hình dữ liệu số. Việc phân quyền truy cập không chặt chẽ, thiếu các quy trình ghi nhận nhật ký truy cập, thiếu kiểm toán đường dẫn dữ liệu và thiếu quy trình phản ứng khi phát hiện sự cố bảo mật làm tăng nguy cơ sai sót và gian lận trong báo cáo tài chính. Đồng thời, năng lực kiểm toán viên trong đánh giá

rủi ro an ninh thông tin và xác minh tính toàn vẹn dữ liệu số chưa đồng đều, đòi hỏi các công ty kiểm toán và cơ quan quản lý phải nâng cao chuẩn mực, hướng dẫn kỹ thuật và năng lực chuyên môn để thực hiện đánh giá hiệu quả hơn.

Ngoài ra, mối liên hệ giữa nhà cung cấp dịch vụ công nghệ thông tin bên thứ ba và doanh nghiệp là một yếu tố thực tiễn quan trọng. Nhiều doanh nghiệp thuê dịch vụ lưu trữ, xử lý báo cáo tài chính trên nền tảng đám mây hoặc sử dụng phần mềm kế toán của bên thứ ba. Trong trường hợp này, trách nhiệm pháp lý và cơ chế kiểm soát dữ liệu cần được làm rõ trong hợp đồng dịch vụ. Thực tế cho thấy, rủi ro an ninh có thể xuất phát từ nhà cung cấp dịch vụ - một điểm yếu mà doanh nghiệp thường đánh giá chưa đầy đủ, dẫn đến nguy cơ rò rỉ thông tin kế toán ngay cả khi doanh nghiệp tự tin về hệ thống nội bộ được bảo vệ.

Cuối cùng, việc thực thi quy định pháp luật và giám sát vẫn còn nhiều thách thức. Mặc dù Nghị định số 13/2023/NĐ-CP tạo khung quyền và nghĩa vụ rõ ràng cho việc xử lý dữ liệu cá nhân, việc hướng dẫn kỹ thuật chi tiết, năng lực thanh tra, cũng như các cơ chế xử phạt khi vi phạm vẫn đang trong quá trình hoàn thiện và triển khai trên thực tế; điều này làm giảm tính răn đe và rõ ràng về trách nhiệm của doanh nghiệp trong một số tình huống cụ thể. Sự bất cập giữa yêu cầu minh bạch tài chính (đòi hỏi công bố thông tin) và yêu cầu bảo mật dữ liệu (đòi hỏi hạn chế, bảo vệ thông tin) đang đặt ra nhu cầu cấp thiết về bộ hướng dẫn, chuẩn mực và công cụ kỹ thuật để giúp doanh nghiệp xác định và thực hiện mức độ công bố hợp lý, đồng thời củng cố hệ thống bảo mật tương ứng.

Tóm lại, thực trạng tại Việt Nam hiện nay là: khung pháp lý và công nghệ hỗ trợ cho cả minh bạch lẫn bảo mật đang phát triển song song; nhưng năng lực triển khai ở cấp doanh nghiệp, đặc biệt tại nhóm SME, cùng với các thách thức về kiểm soát nội bộ, quản lý nhà cung cấp dịch vụ bên thứ ba và năng lực kiểm toán còn hạn chế, dẫn tới khoảng cách đáng kể giữa mục tiêu lý thuyết và thực tiễn. Việc thu hẹp khoảng cách này đòi hỏi sự phối hợp giữa cơ quan quản lý, doanh nghiệp, tổ chức kiểm toán và nhà cung cấp dịch vụ công nghệ thông tin để phát triển các tiêu chuẩn kỹ thuật, hướng dẫn thực hiện và chương trình nâng cao năng lực nhằm đạt được cân bằng bền vững giữa bảo mật và minh bạch thông tin kế toán tài chính.

4. Kiến nghị và giải pháp

Để đạt được cân bằng bền vững giữa bảo mật và minh bạch thông tin kế toán tài chính, cần giải pháp đa tầng, kết hợp chính sách, quản trị, kỹ thuật và nâng cao năng lực con người.

Ở cấp chính sách và thể chế, cơ quan quản lý nên ban hành hướng dẫn thực hành tiêu chuẩn cho doanh nghiệp về phạm vi thông tin cần công bố và kỹ thuật bảo vệ tương ứng, ví dụ: danh mục thông tin bắt buộc công bố, thông tin có thể ẩn danh/khử nhận dạng, đồng thời làm rõ trách nhiệm pháp lý giữa doanh nghiệp và nhà cung cấp dịch vụ bên thứ ba. Nghị định số 13/2023/NĐ-CP đã tạo khuôn khổ cho bảo vệ dữ liệu cá nhân; bước tiếp theo cần là các hướng dẫn kỹ thuật và mẫu hợp đồng tiêu chuẩn để doanh nghiệp áp dụng một cách nhất quán. Sự phối hợp liên ngành (Bộ Tài chính, Bộ TT&TT, Bộ Công an) và kênh tham vấn với doanh nghiệp là cần thiết để hướng dẫn phù hợp với thực tế ngành.

Ở cấp tổ chức, doanh nghiệp cần thiết lập bộ quản trị dữ liệu rõ ràng: phân loại dữ liệu, xác định dữ liệu nào là nhạy cảm/chiến lược, chính sách phân quyền truy cập theo nguyên tắc tối thiểu cần biết, thủ tục ghi nhật ký truy cập và chính sách lưu giữ/xóa dữ liệu. Việc bổ nhiệm một cán bộ chịu trách nhiệm quản trị dữ liệu và xây dựng quy trình ứng phó sự cố là yêu cầu tối thiểu để giảm thiểu rủi ro rò rỉ khi công bố thông tin. Đồng thời, doanh nghiệp cần áp dụng các công cụ kỹ thuật như mã hóa dữ liệu, giải pháp phát hiện xâm nhập, hệ thống quản lý bản ghi và giải pháp bảo vệ dữ liệu để bảo vệ luồng dữ liệu từ khi sinh

ra đến khi công bố. Các biện pháp này không chỉ bảo vệ mà còn tạo ra bằng chứng kiểm toán cần thiết cho kiểm toán viên khi đánh giá tính toàn vẹn của báo cáo tài chính.

Về mặt kỹ thuật và tiêu chuẩn, doanh nghiệp nên hướng tới thiết lập Hệ thống quản lý an toàn thông tin theo tiêu chuẩn quốc tế (ISO/IEC 27001) và thực hiện kiểm toán định kỳ cho hệ thống đó; chứng nhận ISO 27001 hoặc báo cáo kiểm toán bên thứ ba sẽ tăng độ tin cậy cho thông tin công bố mà vẫn bảo đảm biện pháp bảo mật. Cục An toàn thông tin đã cung cấp các hướng dẫn và nền tảng hỗ trợ nhằm giúp các tổ chức xác định cấp độ an toàn hệ thống và triển khai phương án tương ứng; doanh nghiệp nên tận dụng các tài liệu và nền tảng này để triển khai các bước đánh giá, khắc phục lỗ hổng và xây dựng hồ sơ bảo đảm an toàn.

Về kiểm soát nội bộ và kiểm toán, cơ quan quản lý chuyên ngành (Bộ Tài chính) và các hiệp hội nghề nghiệp nên phối hợp với tổ chức kiểm toán để cập nhật hướng dẫn kỹ thuật cho kiểm toán viên trong việc đánh giá dữ liệu số, bao gồm các thủ tục kiểm tra đối với dữ liệu trên nền tảng đám mây, xác minh nhật ký truy cập, và đánh giá rủi ro do nhà cung cấp dịch vụ bên thứ ba. Đồng thời, cần triển khai chương trình đào tạo chuyên sâu cho kiểm toán viên và kế toán nội bộ về kỹ năng phân tích dữ liệu, kiểm toán hệ thống thông tin và pháp luật bảo vệ dữ liệu nhằm đảm bảo tính tin cậy khi doanh nghiệp mở rộng công bố thông tin theo IFRS.

Đối với nhóm doanh nghiệp vừa và nhỏ, cần có gói hỗ trợ thực tiễn: (1) mẫu chính sách, checklist đánh giá rủi ro bảo mật dành cho SME; (2) khuyến khích sử dụng dịch vụ quản trị an ninh thông tin thuê ngoài có chứng nhận; (3) cơ chế hỗ trợ tài chính, ưu đãi thuế hoặc chương trình đào tạo do cơ quan nhà nước cung cấp để giảm gánh nặng chi phí ban đầu. Việc này giúp SME đạt mức bảo mật tối thiểu cần thiết để công bố thông tin tin cậy mà không phải chịu chi phí quá lớn. Cục An toàn thông tin và các đơn vị liên quan đã triển khai một số nền tảng hỗ trợ và tài liệu hướng dẫn, doanh nghiệp nên tận dụng nguồn lực này.

Cuối cùng, cần một lộ trình thực hiện cho từng doanh nghiệp: (1) bước khởi đầu là đánh giá rủi ro thông tin và phân loại dữ liệu; (2) xây dựng chính sách quản trị dữ liệu và phân quyền; (3) áp dụng các biện pháp kỹ thuật cơ bản (mã hóa, backup, SIEM, DLP); (4) thực hiện minh bạch có chọn lọc: soạn thảo "bảng công bố tiêu chuẩn" theo loại hình doanh nghiệp để hướng dẫn báo cáo; (5) nâng cấp lên ISMS/ISO 27001 và báo cáo kiểm toán độc lập khi doanh nghiệp đã có quy mô dữ liệu và công bố lớn hơn. Lộ trình này nên được tích hợp vào tiến trình áp dụng IFRS để đảm bảo yêu cầu minh bạch gia tăng đi kèm với năng lực bảo mật tương ứng ■

TÀI LIỆU THAM KHẢO:

Bộ Tài chính (2015). Luật Kế toán số 88/2015/QH13, Hà Nội.

Bộ Tài chính (2020). Đề án áp dụng Chuẩn mực Báo cáo tài chính quốc tế (IFRS) tại Việt Nam, Hà Nội.

Bộ Thông tin và Truyền thông (2022). Báo cáo an toàn thông tin mạng Việt Nam, Hà Nội.

Chính phủ Nước Cộng hòa xã hội chủ nghĩa Việt Nam (2018). Luật An ninh mạng, Hà Nội.

Chính phủ Nước Cộng hòa xã hội chủ nghĩa Việt Nam (2023). Nghị định số 13/2023/NĐ-CP về bảo vệ dữ liệu cá nhân, Hà Nội.

Hội Kế toán và Kiểm toán Việt Nam (VAA) (2021). Chuẩn mực đạo đức nghề nghiệp kế toán, kiểm toán, Hà Nội.

Nguyễn Văn Công (2019). Hệ thống thông tin kế toán trong doanh nghiệp, Nhà xuất bản Tài chính, Hà Nội.

Trần Thị Minh (2021). Kế toán tài chính trong bối cảnh chuyển đổi số. Nhà xuất bản Kinh tế quốc dân, Hà Nội.

Ủy ban Chứng khoán Nhà nước (2021). Quy định về công bố thông tin trên thị trường chứng khoán, Hà Nội.

Vũ Hữu Đức (2020). Kiểm soát nội bộ trong doanh nghiệp. Nhà xuất bản Kinh tế Quốc dân, Hà Nội.

Ngày nhận bài: 24/11/2025
Ngày phản biện đánh giá và sửa chữa: 20/12/2025
Ngày chấp nhận đăng bài: 30/12/2025

BALANCING SECURITY AND TRANSPARENCY IN FINANCIAL ACCOUNTING INFORMATION AMID DIGITAL TRANSFORMATION IN VIETNAMESE ENTERPRISES

● **TRAN THI VAN**[1]
● **TRAN THI THU HA**[1]
[1]Hai Phong University

ABSTRACT:

In the context of rapid digital transformation across the economy and society, financial accounting faces growing pressure to simultaneously safeguard information security and enhance transparency to meet the expectations of internal management, investors, and regulatory authorities. This study examines the theoretical foundations underlying the relationship between security and transparency in financial accounting information and analyzes how this relationship is manifested in the digital environment. Drawing on an assessment of current practices in Vietnam, the study identifies key challenges arising from technological adoption, data governance, and regulatory compliance that affect both the protection and disclosure of accounting information. The analysis highlights the inherent trade-offs and complementarities between security and transparency, contributing to a clearer understanding of how financial accounting systems can function effectively in the digital era while maintaining credibility, reliability, and trust among stakeholders.

Keywords: information security, information transparency, financial accounting, financial accounting information, digital technology, Vietnamese enterprises.