

# Đánh giá khoảng cách giữa yêu cầu chính sách và năng lực an toàn thông tin tại Hệ thống Quỹ tín dụng nhân dân Việt Nam

Chu Thị Hồng Hải, Phan Thanh Đức, Triệu Thu Hương, Lưu Quang Hà  
Học viện Ngân hàng Việt Nam

Ngày nhận: 18/01/2026

Ngày nhận bản sửa: 01/04/2026

Ngày duyệt đăng: 08/04/2026

*Tóm tắt: Nghiên cứu đo lường khoảng cách giữa ngưỡng yêu cầu tối thiểu tại mốc năm 2025 và năng lực an toàn thông tin thực tế của hệ thống Quỹ tín dụng nhân dân Việt Nam, qua đó rút ra hàm ý cho giai đoạn chuyển đổi số 2026- 2030. Trên mẫu 1.068 quỹ tín dụng nhân dân hợp lệ và khung phân tích kết hợp lý thuyết thể chế với quan điểm dựa trên nguồn lực (RBV), kết quả cho thấy điểm an toàn thông tin trung bình toàn hệ thống đạt 1,89/5,0; 87,73% đơn vị nằm dưới ngưỡng tối thiểu  $E = 2,5$ . Phân rã theo Khung an ninh mạng NIST cho thấy thiếu hụt tập trung ở các năng lực vận hành, đặc biệt là các pha Phát hiện và Phục hồi, trong khi lớp thiết lập/tuân thủ đạt mức cao hơn. Kết quả đồng thời gợi ý sự lệch pha giữa lớp thiết lập/tuân thủ và lớp thực thi vận*

## Assessing the gap between policy requirements and information security capacity in the Vietnam People's Credit Funds system

**Abstract:** This study measures the gap between the minimum required threshold at the 2025 milestone and the actual information security (cybersecurity) capability of Vietnam People's Credit Funds (PCFs) system, thereby drawing implications for the 2026- 2030 digital transformation period. Based on a valid sample of 1,068 PCFs and an analytical framework integrating institutional theory with the resource-based view (RBV), the findings show that the system-wide average information security score is 1.89 out of 5.0, with 87.73% of units falling below the minimum threshold ( $E = 2.5$ ). A decomposition using the NIST Cybersecurity Framework indicates that deficiencies are concentrated in deeper operational capabilities, particularly Detect and Recover, while the establishment/compliance layer performs relatively better. The results also suggest a mismatch between the establishment/compliance layer and the operational execution layer, especially among smaller entities. On that basis, the study recommends shifting the regulatory focus from compliance control to capability building through shared services and a proportionality principle tailored to organizational size.

**Keywords:** Information Security, People's Credit Fund, Policy-Capacity Gap, NIST

Link Doi: <https://doi.org/10.59276/JELB.2026.04.3153>

Chu Thi Hong Hai<sup>1</sup>, Phan Thanh Duc<sup>2</sup>, Trieu Thu Huong<sup>3</sup>, Luu Quang Ha<sup>4</sup>

Email: haict@hvn.edu.vn<sup>1</sup>, ducpt@hvn.edu.vn<sup>2</sup>, huongtrieu@hvn.edu.vn<sup>3</sup>, quangha.hvn@gmail.com<sup>4</sup>

Organization of all: Banking Academy of Vietnam

*hành. Từ đó, nghiên cứu đề xuất chuyển trọng tâm quản lý từ kiểm soát tuân thủ sang kiến tạo năng lực thông qua dịch vụ dùng chung và nguyên tắc tương xứng theo quy mô.*

*Từ khóa: An toàn thông tin, Quĩ tín dụng nhân dân, Khoảng cách năng lực và lý thuyết thể chế, NIST*

**Trích dẫn:** Chu Thị Hồng Hải, Phan Thanh Đức, Triệu Thu Hương, & Lưu Quang Hà. (2026).

Đánh giá khoảng cách giữa yêu cầu chính sách và năng lực an toàn thông tin tại Hệ thống Quĩ tín dụng nhân dân Việt Nam. *Tạp chí Kinh tế - Luật và Ngân hàng*, 28(4), 130-142.

<https://doi.org/10.59276/JELB.2026.04.3153>

## 1. Giới thiệu

Chuyển đổi số (CDS) ngành ngân hàng tại Việt Nam đang chuyển từ giai đoạn tạo lập nền tảng (2021- 2025) sang phát triển chiều sâu (2026- 2030), trong đó an toàn thông tin (ATTT) trở thành điều kiện quan trọng cho tăng trưởng bền vững (Ngân hàng Nhà nước, 2021). Việc mở rộng hệ sinh thái số qua các kênh giao dịch và kết nối API giúp gia tăng tiện ích, nhưng đồng thời cũng làm mở rộng bề mặt tấn công và gia tăng rủi ro ATTT (Verizon, 2024).

Trong bối cảnh này, Quĩ tín dụng nhân dân (QTDND)- một định chế tài chính hợp tác quy mô nhỏ- đang đối mặt với áp lực ATTT ngày càng lớn khi hội nhập sâu hơn vào hạ tầng thanh toán quốc gia. Do hạn chế về nguồn lực và nhân sự công nghệ so với các ngân hàng thương mại, sự cố ATTT tại QTDND không chỉ gây thiệt hại nội bộ mà còn có nguy cơ tạo ra hiệu ứng lan truyền rủi ro qua các điểm kết nối kỹ thuật của hệ thống tài chính (Brando và cộng sự, 2022; Lee và cộng sự, 2025).

Thực tiễn cho thấy hệ thống QTDND đang rơi vào tình huống “rủi ro kép”: chịu áp lực mạnh mẽ phải số hóa để thích ứng, nhưng lại thiếu hụt nền tảng nguồn lực như nhân sự, công nghệ và quản trị để bảo đảm ATTT (Ngân hàng Hợp tác xã Việt Nam, 2025). Sự bất cân xứng này làm gia tăng tính dễ

tổn thương trước các đe dọa mạng, tương đồng với thực trạng của nhiều tổ chức tài chính nhỏ tại các nền kinh tế đang phát triển (Kshetri, 2013; Opoku và cộng sự, 2025).

Dưới lăng kính Lý thuyết Thể chế, áp lực quản lý có thể thúc đẩy tổ chức thiết lập các quy trình mang tính hình thức nhằm đạt tính chính danh, song mức độ chuyển hóa thành năng lực thực chất lại phụ thuộc vào điều kiện nguồn lực nội tại (Meyer & Rowan, 1977; DiMaggio & Powell, 1983; Hsu và cộng sự, 2012). Điều này gợi ý khả năng tồn tại hiện tượng “tách rời” (decoupling), tức khoảng cách giữa lớp thiết lập/tuân thủ chính sách và lớp thực thi vận hành ATTT.

Tại Việt Nam, các nghiên cứu về rủi ro an ninh mạng trong lĩnh vực tài chính hiện chủ yếu tập trung vào khối ngân hàng thương mại (Nguyen và cộng sự, 2020; Tam và cộng sự, 2020), trong khi bằng chứng định lượng về khoảng cách giữa yêu cầu chính sách và năng lực ATTT của hệ thống QTDND vẫn còn hạn chế. Để lấp đầy khoảng trống này, nghiên cứu sử dụng dữ liệu khảo sát từ 1.068 QTDND, bao phủ 90,8% toàn hệ thống. Trên cơ sở đó, nghiên cứu trả lời ba câu hỏi cốt lõi: (RQ1) khoảng cách giữa ngưỡng yêu cầu chính sách tối thiểu và năng lực ATTT thực tế của hệ thống QTDND hiện ở mức nào; (RQ2) liệu có tồn tại chênh lệch có ý nghĩa giữa mức độ tuân thủ quy trình và năng lực vận hành ATTT hay không; và (RQ3)

Đánh giá khoảng cách giữa yêu cầu chính sách và năng lực an toàn thông tin  
 tại Hệ thống Quỹ tín dụng nhân dân Việt Nam

những hàm ý chính sách nào có thể giúp củng cố ATTT bền vững cho QTDND giai đoạn 2026- 2030. Nghiên cứu kỳ vọng cung cấp cơ sở thực chứng cho việc chuyển dịch từ “kiểm soát tuân thủ” sang “kiến tạo năng lực” đối với các tổ chức hạn chế nguồn lực (Gordon và cộng sự, 2011; National Institute of Standards and Technology, 2016).

## 2. Cơ sở lý thuyết và tổng quan nghiên cứu

### 2.1. Cơ sở lý thuyết

Nghiên cứu tiếp cận ATTT như một năng lực tổ chức bảo đảm vận hành an toàn và khả năng ứng phó, thay vì như tập hợp các giải pháp kỹ thuật rời rạc. Theo quan điểm dựa trên nguồn lực (RBV), năng lực này được hình thành từ sự tích lũy và phối hợp các nguồn lực then chốt. Trong đó, “giá trị” thể hiện ở khả năng duy trì liên tục hoạt động, còn tính “khó sao chép” nằm ở kỹ luật vận hành và năng lực học tập- cải tiến hơn là ở các công cụ có thể mua ngoài (Barney, 1991). Vì vậy, khi nguồn lực nền tảng hạn chế, tổ chức khó duy trì kỹ luật và cải tiến liên tục- những thành tố cốt lõi của mức độ trưởng thành an ninh mạng.

Bổ sung cho RBV, Lý thuyết Thể chế giải thích cách tổ chức phản ứng trước áp lực chuẩn hóa. Để đạt được tính chính danh (legitimacy), các tổ chức có thể ưu tiên thiết lập các cấu trúc hình thức (quy chế, hồ sơ tuân thủ) trong khi thực thi chưa tương xứng- hiện tượng “tách rời” (Meyer & Rowan, 1977). Dưới áp lực đồng hình, các tổ chức có xu hướng “giống nhau” về văn bản chính sách nhưng khác biệt về hiệu quả thực chất do chênh lệch nguồn lực (DiMaggio & Powell, 1983). Do đó, “có chính sách” chưa đồng nghĩa với “có năng lực thực thi”, bởi việc triển khai còn chịu chi phối bởi nhận thức rủi ro và cơ chế kiểm soát nội tại (Bulgurcu và cộng sự, 2010; Hsu và cộng sự, 2012).

Sự kết hợp hai lăng kính này tạo nên một khung giải thích nhất quán cho nghịch lý “tuân thủ nhưng thiếu năng lực”: áp lực thể chế thúc đẩy điểm số chính sách, trong khi ràng buộc nguồn lực kìm hãm năng lực thực thi. Từ đó hình thành khoảng cách (gap) giữa yêu cầu và thực tế, làm cơ sở cho việc thiết kế thước đo nghiên cứu.

### 2.2. Tổng quan nghiên cứu

Các dòng nghiên cứu liên quan đề cập nhiều ở ba điểm chính. Thứ nhất, về mức độ dễ bị tấn công, các tổ chức tài chính quy mô nhỏ có xu hướng dễ tổn thương hơn do hạn chế về giám sát, nhân lực và đầu tư bảo vệ; vì vậy, các cuộc tấn công mạng thường tập trung vào các mục tiêu có “độ phòng vệ thấp”, làm gia tăng nguy cơ gián đoạn vận hành và ảnh hưởng đến tính liên tục của dịch vụ (Kshetri, 2013; Adejumo & Ogburie, 2025; Opoku và cộng sự, 2025). Tuy nhiên, phần lớn nghiên cứu hiện hành vẫn thiên về mô tả bối cảnh và nhóm rủi ro, chưa cung cấp bằng chứng định lượng cấp hệ thống về mức độ thiếu hụt theo từng chức năng kiểm soát/ứng phó trong các mô hình hợp tác tương đồng QTDND.

Thứ hai, về phương pháp đo lường, các khung đánh giá năng lực/mức trưởng thành được sử dụng để chuẩn hóa việc so sánh và ưu tiên can thiệp, đặc biệt theo hướng tối thiểu khả thi và triển khai theo giai đoạn đối với các tổ chức hạn chế nguồn lực (National Institute of Standards and Technology, 2016; Rea-Guaman và cộng sự, 2017). Các nghiên cứu so sánh mô hình trưởng thành cho thấy sự đa dạng khung đo và gợi ý nhu cầu lựa chọn thước đo phù hợp mục tiêu quản trị và bối cảnh nguồn lực (Rea-Guaman và cộng sự, 2017; Proença & Borbinha, 2018). Trong các bối cảnh hạn chế nguồn lực, cách tiếp cận theo “khoảng cách” giữa chuẩn kỳ vọng và mức thực thi thực tế được xem là thực

dụng để định vị vùng thiếu hụt cần ưu tiên (Lee và cộng sự, 2025; National Institute of Standards and Technology, 2016). Tuy vậy, các nghiên cứu đối sánh theo quy chiếu chính sách cụ thể ở cấp hệ thống cho nhóm tổ chức tài chính quy mô nhỏ vẫn còn hạn chế.

Thứ ba, về hàm ý giải pháp, chi phí và tổn thất kinh tế do sự cố ATTT đặt ra yêu cầu tối ưu hóa hiệu quả đầu tư; do đó, đối với các tổ chức quy mô nhỏ, việc dựa hoàn toàn vào mô hình “tự cung tự cấp” thường khó khả thi khi năng lực triển khai và duy trì kiểm soát vận hành sâu còn hạn chế (Gordon và cộng sự, 2011; Antunes và cộng sự, 2021). Các nghiên cứu cũng cho thấy việc nâng cao năng lực thường gắn với chuẩn hóa quy trình, tăng cường kỷ luật vận hành và tận dụng cơ chế hỗ trợ bên ngoài/đơn vị trung gian (Antunes và cộng sự, 2021; National Institute of Standards and Technology, 2016; Cartwright và cộng sự, 2023).

Từ tổng quan trên, nghiên cứu xác định ba khoảng trống cần lấp đầy: (i) thiếu bằng chứng định lượng diện rộng về năng lực ATTT tại khu vực tài chính quy mô nhỏ ở Việt Nam, đặc biệt là hệ thống QTDND; (ii) thiếu cách tiếp cận đo lường khoảng cách dựa trên quy chiếu chính sách cụ thể ở cấp hệ thống; và (iii) thiếu bằng chứng thực nghiệm ở cấp hệ thống về sự lệch pha giữa lớp thiết lập/tuân thủ và lớp thực thi vận hành, trong đó các nghiên cứu hiện có chưa kiểm định đầy đủ sự lệch pha giữa lớp thiết lập/tuân thủ và lớp thực thi vận hành trên dữ liệu cấp hệ thống.

### 2.3. Khung phân tích GAP

Nghiên cứu vận hành hóa khung phân tích GAP bằng cách đối sánh hai đại lượng trên cùng thang đo khảo sát. Kỳ vọng (Target) được xác lập dựa trên việc quy chiếu các yêu cầu chính sách ngành ngân hàng sang các chỉ báo đo lường và mã hóa theo cùng

hệ chỉ báo/thang đo sử dụng trong khảo sát, nhằm bảo đảm ngưỡng so sánh có căn cứ và hạn chế tính tùy ý trong lựa chọn ngưỡng so sánh.

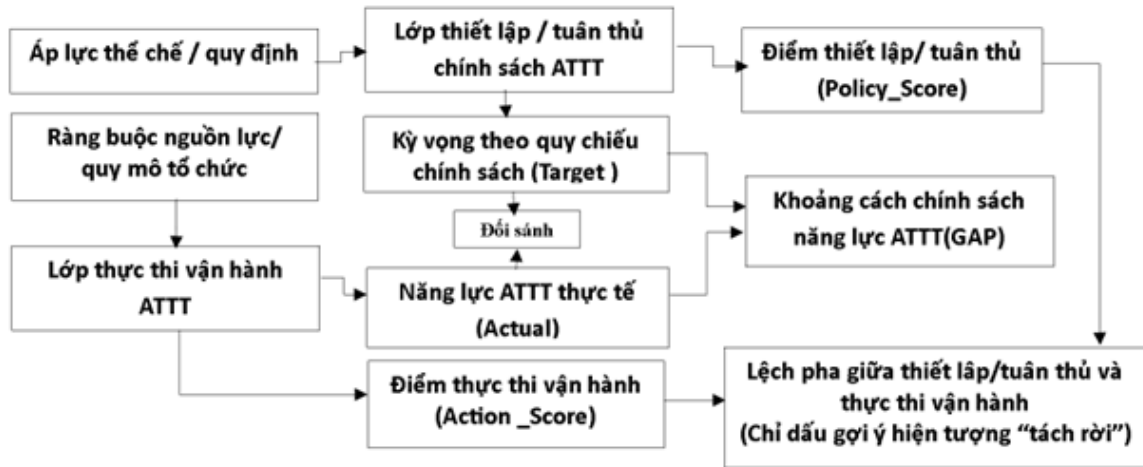
Năng lực thực tế (Actual) là điểm đánh giá hiện trạng của từng đơn vị theo cùng hệ chỉ báo. Khoảng cách năng lực được tính theo công thức  $GAP = Actual - Target$ ; khi  $GAP < 0$ , đơn vị được xác định là thiếu hụt năng lực và thuộc vùng ưu tiên can thiệp, còn độ lớn  $|GAP|$  phản ánh mức độ nghiêm trọng của thiếu hụt.

Theo cách tiếp cận của nghiên cứu, Target mang tính quy chiếu chuẩn mực còn Actual phản ánh hiện trạng từ khảo sát; do đó, nghiên cứu sử dụng cùng cấu trúc thang đo để tăng tính tương thích khi đối sánh. GAP là chỉ số chẩn đoán mức thiếu hụt, không tự thân phân biệt cơ chế hình thành khoảng cách. Vì vậy, cơ chế được diễn giải thông qua các phân tích bổ trợ, thay vì suy luận trực tiếp từ công thức GAP.

### 2.4. Khung phân tích nghiên cứu

Trên nền tảng tích hợp RBV và Lý thuyết Thể chế, nghiên cứu xây dựng khung phân tích (Hình 1) nhằm: (i) lượng hóa khoảng cách giữa yêu cầu chính sách và năng lực thực tế; và (ii) nhận diện chỉ dấu của sự “tách rời”. Theo đó, áp lực chuẩn hóa từ quy định tạo động lực hình thành chính sách nền, trong khi ràng buộc nguồn lực chi phối mức độ tích hợp vào vận hành.

Dựa trên cấu trúc này, RQ1 được trả lời thông qua đối sánh giữa Target và Actual; RQ2 được xem xét gián tiếp qua chênh lệch giữa điểm thiết lập (Policy\_Score) và điểm vận hành (Action\_Score). Sự lệch pha này được xem như một chỉ dấu thực nghiệm của hiện tượng tách rời. Khung phân tích không nhằm kiểm định một mô hình nhân quả đầy đủ, mà đóng vai trò cơ sở lý thuyết cho đo lường và diễn giải kết quả. RQ3



Nguồn: Nhóm tác giả đề xuất trên nền tảng RBV và lý thuyết thể chế và khung phân tích GAP

Hình 1. Khung phân tích nghiên cứu

(hàm ý chính sách) được đúc kết từ kết quả của RQ1 và RQ2, do đó không nằm trong cấu trúc của khung phân tích.

### 3. Phương pháp nghiên cứu

#### 3.1. Thiết kế nghiên cứu

Nghiên cứu sử dụng thiết kế định lượng cắt ngang dựa trên khảo sát quy mô hệ thống theo tiếp cận gần tổng điều tra, phù hợp với mục tiêu đo lường thực trạng và đối sánh năng lực tại một thời điểm quan sát; thiết kế này thích hợp cho mô tả hiện trạng, xác lập đường cơ sở và xem xét các liên hệ thực chứng, nhưng không nhằm suy luận nhân quả (Setia, 2016). Trên cơ sở dữ liệu đó, nghiên cứu phân tích khoảng cách (GAP) giữa ngưỡng yêu cầu tối thiểu và năng lực thực tế theo logic quản trị rủi ro, đồng thời xem xét sự lệch pha giữa nhóm chỉ báo phản ánh lớp thiết lập/tuân thủ và nhóm chỉ báo phản ánh lớp thực thi vận hành (National Institute of Standards and Technology, 2016). Cách tiếp cận đánh giá dựa trên chuẩn kiểm soát để nhận diện thiếu hụt và định hướng cải thiện cũng đã được áp dụng trong nghiên cứu ATTT cấp

tổ chức (Antunes và cộng sự, 2021). Vì vậy, các diễn giải về cơ chế trong bài chỉ được hiểu theo hướng gợi ý và hỗ trợ thảo luận.

#### 3.2. Dữ liệu, mẫu nghiên cứu và quy trình thu thập

Dữ liệu sử dụng là dữ liệu sơ cấp gốc từ cuộc khảo sát cắt ngang về mức độ CDS của hệ thống QTDND do nhóm nghiên cứu trực tiếp xây dựng công cụ, tổ chức thu thập, làm sạch và phân tích vào tháng 6/2025; Ngân hàng Hợp tác xã Việt Nam (NHHTX) (Co-opBank) phối hợp triển khai, hướng dẫn và đôn đốc các đơn vị tham gia. Mục tiêu khảo sát là đánh giá mức độ CDS của hệ thống tại thời điểm khảo sát, bộ dữ liệu dùng trong bài là bộ dữ liệu gốc. Bảng hỏi được phát triển qua 7 phiên bản, tham vấn chuyên gia qua 3 vòng (V1: xây dựng 8 trụ cột; V2: bộ công cụ ban đầu; V3: bộ công cụ sau khảo sát thử) và khảo sát thử tại 3 QTDND có quy mô, địa bàn khác nhau. Khảo sát chính thức được thực hiện trực tuyến; các QTDND được cấp mã số, nhận bộ câu hỏi chính thức, tham gia tập huấn trực tuyến toàn hệ thống và trả lời thử trong 3 ngày trước khi hệ thống được thiết lập lại để khảo sát chính thức trong 7

ngày. Trong suốt quá trình này, NHHTX và nhóm nghiên cứu bố trí nhân sự hỗ trợ nhằm bảo đảm thông tin phản ánh sát thực trạng CDS của hệ thống QTDND. Khảo sát thu 1.076 phiếu; sau làm sạch còn 1.068 quan sát hợp lệ trên 1.176 QTDND đang hoạt động, tương ứng mức bao phủ 90,8%. Mỗi quan sát được tổng hợp ở cấp QTDND từ hai nhóm trả lời theo thiết kế gồm lãnh đạo/ban điều hành và cán bộ nghiệp vụ; chỉ các đơn vị hoàn thành đầy đủ thông tin bắt buộc mới được chấp nhận là hợp lệ. Bộ dữ liệu khảo sát đã được đơn vị chủ trì cho phép sử dụng cho mục đích nghiên cứu.

### 3.3. Thang đo, đo lường biến và độ tin cậy

Bộ công cụ khảo sát gồm 8 trụ cột (TC1-TC8), phục vụ đánh giá tổng thể mức độ CDS của QTDND. Trong nghiên cứu này, các trụ cột được lựa chọn theo mức độ gắn trực tiếp với khung nghiên cứu đề xuất, thay vì sử dụng toàn bộ như các biến độc lập trong cùng một mô hình kiểm định. Cụ thể, năng lực ATTT thực tế (Actual) được đo bằng trụ cột TC4- An ninh và Bảo mật (gồm 16 biến quan sát); ràng buộc nguồn lực được phản ánh chủ yếu qua TC1 (Nhân lực và nhận thức) và TC7 (Nguồn lực tài chính và hợp tác). Trong khi đó, áp lực thể chế/quy định không được đo như một biến độc lập riêng, mà được quy chiếu vào phần Target và sử dụng như cơ sở diễn giải trong khung phân tích.

Nội dung TC4 được tổ chức theo 5 chức năng an ninh mạng của NIST gồm Nhận diện- Bảo vệ- Phát hiện- Ứng phó- Phục hồi (National Institute of Standards and Technology, 2016). Các biến quan sát được chấm theo thang 0–5 (0 = chưa triển khai; 5 = tối ưu). Từ điểm thành phần, nghiên cứu tính điểm trung bình tổng hợp và quy chiếu theo 5 mức trưởng thành tổng quát: M1: 0–1 điểm; M2: >1–2 điểm; M3: >2–3

điểm; M4: >3–4 điểm; M5: >4–5 điểm. Do mục tiêu của bài là đo lường và đối sánh năng lực ở cấp hệ thống, TC4 được sử dụng như một chỉ số tổng hợp phục vụ chẩn đoán. Độ tin cậy nội tại của thang đo được đánh giá bằng Cronbach's Alpha; kết quả cho thấy TC4 đạt  $\alpha = 0,935$ , phản ánh mức nhất quán nội tại rất cao và đủ cơ sở cho các phân tích tiếp theo.

### 3.4. Khung phân tích khoảng cách và chiến lược kiểm định “tách rời”

Ngưỡng kỳ vọng tối thiểu E (Target) được xác lập theo nguyên tắc quy chiếu mục tiêu chính sách vào cùng hệ chỉ báo và cùng thang mức triển khai sử dụng trong khảo sát. Cụ thể, Quyết định 810/QĐ-NHNN năm 2021 (Phê duyệt “Kế hoạch chuyển đổi số ngành Ngân hàng đến năm 2025, định hướng đến năm 2030”) quy định các yêu cầu CDS trong ngành Ngân hàng theo từng nhóm nội dung và kèm theo tỷ lệ (%) mục tiêu theo lộ trình thực hiện (Ngân hàng Nhà nước, 2021), trong khi Quyết định 2158/QĐ-BTTTT ngày 07/11/2023 (Quyết định Phê duyệt Đề án xác định chỉ số đánh giá mức độ chuyển đổi số doanh nghiệp và hỗ trợ thúc đẩy doanh nghiệp chuyển đổi số) cung cấp khung đánh giá mức độ CDS theo 5 mức, trong đó mỗi mức gắn với tỷ lệ hoàn thành tiêu chí tương ứng để phân loại mức đạt (Bộ Thông tin và Truyền thông, 2023). Trên cơ sở đối sánh hai khung này, nghiên cứu quy đổi về cùng thang điểm khảo sát và xác định ngưỡng tối thiểu cần đạt tại mốc năm 2025 là  $E = 2,5$ . Theo cách tiếp cận này, Target không phải là thang đo độc lập được thu thập riêng, mà là ngưỡng quy chiếu được mã hóa về cùng hệ chỉ báo với Actual.

Khoảng cách năng lực được xác định bằng công thức:  $GAP = Actual - E$ . Khi  $GAP < 0$ , đơn vị bị đánh giá là thiếu hụt năng lực; trong khi  $|GAP|$  phản ánh mức độ nghiêm trọng

Đánh giá khoảng cách giữa yêu cầu chính sách và năng lực an toàn thông tin

tại Hệ thống Quỹ tín dụng nhân dân Việt Nam

của thiếu hụt. Cách tiếp cận này thống nhất với logic quản trị rủi ro của NIST (2016), theo đó việc đánh giá tác động, nhận diện lỗ hổng và ưu tiên xử lý được thực hiện trên cơ sở so sánh giữa yêu cầu bảo vệ và mức độ đáp ứng thực tế. Ở góc độ thực chứng, cách tiếp cận đánh giá dựa trên bộ kiểm soát (controls) để chẩn đoán mức độ đáp ứng và định hướng cải thiện cũng đã được áp dụng trong các nghiên cứu ATTT cấp tổ chức, chẳng hạn Antunes và cộng sự (2021).

Đối với RQ2, dựa trên sự phân định của NIST (2016) giữa policy và procedure, nghiên cứu chia các biến TC4 thành hai nhóm: (a) nhóm thiết lập/tuân thủ (Policy\_Score) gồm quy chế, quy trình và hồ sơ; và (b) nhóm thực thi vận hành (Action\_Score) gồm giám sát, phát hiện, diễn tập, ứng cứu và phục hồi. Điểm trung bình của hai nhóm được so sánh cặp (paired t-test) kèm kích thước ảnh hưởng. Sự chênh lệch có ý nghĩa thống kê không được xem là bằng chứng trực tiếp của cơ chế “tách rời”, mà chỉ đóng vai trò như một chỉ dấu thực nghiệm gợi ý về sự lệch pha giữa hồ sơ tuân thủ và vận hành thực tiễn.

Đối với RQ3, nghiên cứu xem xét vai trò của ràng buộc nguồn lực bằng cách đối chiếu mức thiếu hụt (GAP) của TC4 với các trụ cột điều kiện nền, đặc biệt là TC1 và TC7. Kết hợp với phân tích phân tầng theo quy mô, kết quả này tạo cơ sở thực chứng để rút ra các hàm ý can thiệp ở cấp hệ thống trong phần thảo luận.

#### 4. Kết quả nghiên cứu và phân tích

##### 4.1. Kiểm định độ tin cậy dữ liệu và xác lập đường cơ sở năng lực an toàn thông tin

Sau bước làm sạch dữ liệu, nghiên cứu giữ lại 1.068 QTDND hợp lệ từ 1.076 phiếu thu về. Các phiếu bị loại chủ yếu do thiếu một trong hai nhóm trả lời theo thiết kế hoặc thiếu thông tin bắt buộc để tính các chỉ số nghiên cứu. Trên nền dữ liệu đã làm sạch, nghiên cứu đánh giá độ tin cậy nội tại của bộ chỉ báo nhằm bảo đảm cơ sở cho các phân tích mô tả và đối sánh tiếp theo. Bộ công cụ khảo sát là công cụ gốc do nhóm tác giả phát triển, gồm 8 trụ cột và 95 biến quan sát. Do giới hạn dung lượng, bảng hỏi chi tiết

**Bảng 1. Cấu trúc thang đo DMI và độ tin cậy nội tại**

Trụ cột đo lường	Số biến quan sát	Cronbach's alpha	Nội dung đo lường chính
An ninh và Bảo mật (TC4)	16	0,935	Tuân thủ bảo mật thông tin và năng lực quản trị rủi ro
Hạ tầng và Kết nối (TC3)	13	0,840	Hệ thống phần mềm lõi, thiết bị phần cứng và kết nối mạng
Dữ liệu và Phân tích (TC5)	13	0,790	Năng lực thu thập, lưu trữ, phân tích và sử dụng dữ liệu
Trải nghiệm khách hàng (TC8)	9	0,726	Mức độ hài lòng, hỗ trợ người dùng, tiếp cận dịch vụ số
Thể chế và quy trình (TC2)	13	0,720	Mức độ chuẩn hóa quy trình, số hóa văn bản và vận hành
Nguồn lực tài chính và hợp tác (tc7)	9	0,710	Khả năng đầu tư công nghệ, tiếp cận hỗ trợ chính sách
Nhân lực & nhận thức (TC1)	12	0,700	Định hướng chiến lược, cam kết và nhận thức số của lãnh đạo
Sản phẩm và dịch vụ số (TC6)	10	0,527	Mức độ số hóa sản phẩm, đa dạng hóa kênh phân phối

*Nguồn: Kết quả xử lý số liệu khảo sát, 2025*

không trình bày đầy đủ trong bài nhưng có thể được cung cấp bởi tác giả liên hệ theo yêu cầu hợp lý nhằm phục vụ mục đích học thuật. Thông tin khái quát về bộ công cụ được trình bày ở Bảng 1.

Kết quả Cronbach's Alpha cho thấy bộ chỉ báo nhìn chung đạt độ tin cậy chấp nhận được đến cao. Trong đó, trụ cột An ninh và Bảo mật (TC4)- biến số trung tâm của nghiên cứu- đạt  $\alpha = 0,935$ , phản ánh mức nhất quán nội tại rất cao giữa các biến quan sát. Trụ cột Sản phẩm & Dịch vụ số (TC6) có hệ số thấp hơn; tuy nhiên, do TC6 không tham gia trực tiếp vào khung phân tích ATTT, điều này không ảnh hưởng đến các kết luận trọng tâm.

Trên nền dữ liệu đạt độ tin cậy, nghiên cứu xác lập đường cơ sở về năng lực ATTT của hệ thống QTDND năm 2025. Kết quả cho thấy điểm ATTT trung bình toàn hệ thống đạt 1,891/5,0 (SD = 0,563), dao động từ 0,188 đến 4,000. So với ngưỡng quy chiếu tối thiểu E = 2,5, mức chênh lệch trung bình là -0,609; đồng thời, 87,73% QTDND có điểm dưới ngưỡng này. Theo cách tiếp cận của nghiên cứu, đây là chỉ báo cảnh báo mức thiếu hụt so với ngưỡng kỳ vọng, không phải kiểm định giả thuyết về trung bình tổng thể.

Đặt ATTT trong bối cảnh các điều kiện nền của CDS cho thấy thiếu hụt không diễn ra đơn lẻ. Khi đối sánh các trụ cột liên quan trực tiếp đến khung phân tích, mức thiếu hụt về nguồn lực tài chính và hạ tầng/kết nối còn lớn hơn thiếu hụt ATTT. Kết quả

**Bảng 2. Thống kê mô tả điểm ATTT (TC4) của hệ thống QTDND**

Chi tiêu	Giá trị
Số QTDND hợp lệ (N)	1.068
Điểm ATTT TC4 trung bình (A)	1,891
Độ lệch chuẩn (SD)	0,563
Trung vị (Median)	1,881
Min- Max	0,188- 4,000
Tỷ lệ QTDND dưới ngưỡng E = 2,5	87,73%
GAP hệ thống (A - E)	-0,609

*Nguồn: Kết quả xử lý số liệu khảo sát, 2025.*

này được sử dụng như bối cảnh thực chứng cho phần thảo luận về tính khả thi của các can thiệp ở cấp hệ thống, thay vì hàm ý quan hệ nhân quả trực tiếp.

#### 4.2. Cấu trúc thiếu hụt theo NIST và chỉ dấu thực nghiệm về sự lệch pha

Nghiên cứu phân rã TC4 theo 5 chức năng tham chiếu của khung NIST (Identify- Protect- Detect- Respond- Recover) nhằm nhận diện thiếu hụt trong chu trình năng lực ATTT.

Kết quả cho thấy thiếu hụt không phân bố đồng đều giữa các chức năng. Nhận diện là chức năng duy nhất vượt ngưỡng tối thiểu (A = 2,978), trong khi Phát hiện và Phục hồi là hai điểm thiếu hụt lớn nhất. Điều này gợi ý điểm yếu nổi bật ở các năng lực giám sát, phát hiện và khôi phục, trong khi lớp

**Bảng 3. Khoảng cách năng lực theo các trụ cột liên quan khung phân tích**

Trụ cột	A (Thực tế)	E (Kỳ vọng)	GAP (A - E)
Nguồn lực tài chính và hợp tác (TC7)	1,38	2,50	-1,12
Hạ tầng và Kết nối (TC3)	1,51	2,50	-0,99
An ninh và Bảo mật (TC4)	1,89	2,50	-0,61
Thể chế và Quy trình (TC2)	1,89	2,50	-0,61
Nhân lực và nhận thức (TC1)	1,94	2,50	-0,56

*Nguồn: Kết quả xử lý số liệu khảo sát, 2025.*

Đánh giá khoảng cách giữa yêu cầu chính sách và năng lực an toàn thông tin  
 tại Hệ thống Quỹ tín dụng nhân dân Việt Nam

**Bảng 4. Điểm ATTT theo 5 chức năng NIST  
 và khoảng cách**

Nhóm chức năng (NIST)	Điểm TB (A)	SD	GAP (A- 2,5)
Identify (Nhận diện)	2,978	0,687	0,478
Protect (Bảo vệ)	2,038	0,593	-0,462
Detect (Phát hiện)	0,731	0,726	-1,769
Respond (Ứng phó)	1,729	0,877	-0,771
Recover (Phục hồi)	1,077	0,739	-1,423

*Nguồn: Kết quả xử lý số liệu khảo sát, 2025*



**Hình 2. Biểu đồ điểm trung bình  
 theo 5 chức năng NIST**

nhận diện và thiết lập yêu cầu được hình thành tương đối tốt hơn.

Để xem xét chỉ dấu gợi ý cho sự lệch pha giữa lớp thiết lập/tuân thủ và lớp thực thi vận hành, nghiên cứu xây dựng hai chỉ số tổng hợp ở cấp từng QTDND: Policy\_Score (trung bình của Identify và Protect) đại diện cho lớp thiết lập/tuân thủ, và Action\_Score (trung bình của Detect, Respond, Recover)

đại diện cho lớp thực thi vận hành. Kết quả kiểm định paired-samples t-test cho thấy Policy\_Score cao hơn Action\_Score một cách nhất quán và có ý nghĩa thống kê rất cao. Chênh lệch trung bình đạt 1,329 điểm, kèm kích thước ảnh hưởng rất lớn (Cohen’s  $d_z = 2,74$ ), cho thấy mức chênh lệch lớn giữa hai lớp chức năng trong mẫu khảo sát. Trong phạm vi thiết kế của nghiên cứu, kết quả này được diễn giải như bằng chứng định lượng mạnh về chênh lệch giữa hai lớp chức năng thiết lập/tuân thủ và lớp thực thi vận hành, đồng thời là gợi ý cho “nghịch lý tuân thủ” hoặc hiện tượng “tách rời” theo nghĩa rộng. Tuy nhiên, kết quả không được hiểu là bằng chứng trực tiếp về áp lực thể chế, động cơ trình diễn tuân thủ hay sự tách biệt có chủ đích.

**4.3. Phân bố năng lực an toàn thông tin**

**Bảng 5. Kiểm định sự khác biệt giữa Policy\_Score và Action\_Score**

Chỉ số tổng hợp	Mean	SD
Điểm chính sách* (Nhận diện + Bảo vệ) /Policy_Score *(Identify + Protect)	2,508	0,568
Điểm hành động* (Phát hiện + Ứng phó + Phục hồi)/ Action_Score *(Detect + Respond + Recover)	1,179	0,668
Chênh lệch trung bình (Chính sách- Hành động)/ Mean Difference (Policy – Action)	1,329	0,485
t(1067)	89,56	
Gía trị p	< 0,001	
Cỡ ảnh hưởng Cohen’s $d_z$ *	2,74	

*Nguồn: Kết quả xử lý số liệu khảo sát, 2025*

**Bảng 6. Phân bố năng lực ATTT (TC4) của hệ thống QTDND**

Mức năng lực ATTT	Định nghĩa trạng thái	Ngưỡng điểm TC4	Số lượng (n)	Tỷ lệ (%)
1	Thụ động / Sơ khai	< 1,5	256	23,97
2	Tuân thủ hình thức / Kế hoạch	1,5- < 2,5	681	63,76
3	Đã xác lập / Vận hành cơ bản	2,5- < 3,5	126	11,80
4	Được quản trị / Đo lường	3,5- < 4,5	5	0,47
5	Tối ưu hóa	≥ 4,5	0	0,00

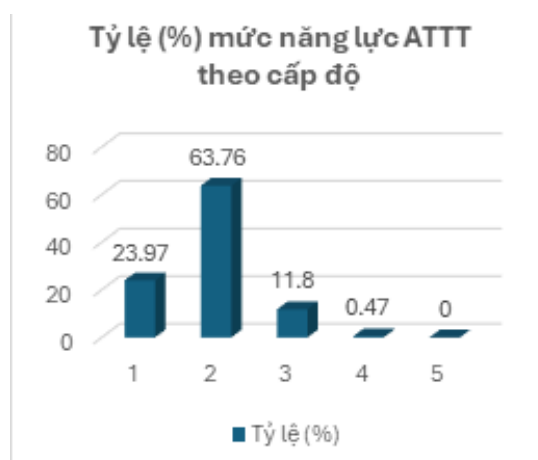
Nguồn: Kết quả xử lý số liệu khảo sát, 2025

Bên cạnh giá trị trung bình, phân bố theo các nhóm khoảng điểm quanh ngưỡng quy chiếu tối thiểu cho phép nhận diện rõ hơn mức độ tập trung của năng lực ATTT trong toàn hệ thống. Trên cơ sở điểm TC4 của từng QTDND và ngưỡng quy chiếu tối thiểu  $E = 2,5$ , nghiên cứu chia mẫu thành 5 nhóm khoảng điểm với các ngưỡng cắt nhất quán: M1 < 1,5; M2: 1,5–<2,5; M3: 2,5–<3,5; M4: 3,5–<4,5; M5  $\geq 4,5$ . Cách chia này nhằm phục vụ phân tích phân bố năng lực quanh ngưỡng tối thiểu E.

Kết quả cho thấy phân bố nghiêng mạnh về vùng dưới ngưỡng tối thiểu: 87,73% đơn vị nằm dưới  $E = 2,5$ , trong khi tỷ lệ đạt từ Mức 3 trở lên chỉ chiếm 12,27% và Mức 4- 5 hầu như không đáng kể. Điều này cho thấy năng lực ATTT của hệ thống chủ yếu vẫn nằm dưới ngưỡng kỳ vọng tối thiểu.

Tuy nhiên, cách phân nhóm theo khoảng điểm quanh ngưỡng  $E = 2,5$  chỉ phản ánh mặt bằng năng lực tổng hợp ở cấp hệ thống, không thay thế cho chẩn đoán theo từng chức năng. Vì vậy, kết quả ở mục này chủ yếu được sử dụng để mô tả phân bố tổng thể của năng lực ATTT, trong khi phân tích theo chức năng được dùng để nhận diện các điểm thiếu hụt trọng yếu.

#### 4.4. Khác biệt theo miền và quy mô- dấu hiệu phân tầng rủi ro và cơ sở cho nguyên tắc tương xứng



**Hình 3. Biểu đồ điểm trung bình theo 5 chức năng NIST**

Để quan sát sự phân bố thiếu hụt ATTT theo vùng địa lý và quy mô tài sản, nghiên cứu xem xét điểm TC4 theo từng nhóm. Kết quả theo miền cho thấy mức biến thiên nhỏ: điểm trung bình dao động từ 1,857 đến 1,914, trong khi tỷ lệ dưới ngưỡng tối thiểu đều rất cao. Mẫu hình này cho thấy thiếu hụt ATTT xuất hiện khá phổ biến trên toàn hệ thống hơn là tập trung ở một vùng cụ thể. Ở một số năng lực vận hành sâu, đặc biệt Phục hồi, Miền Trung có mức điểm thấp hơn tương đối, qua đó gợi ý khác biệt mô tả cần được lưu ý khi xác định ưu tiên can thiệp. Ở góc độ quy mô, dữ liệu cho thấy dấu hiệu phân tầng rõ hơn. Nhóm QTDND dưới 100 tỷ có điểm TC4 thấp nhất và tỷ lệ dưới ngưỡng cao nhất; nhóm này cũng có mức điểm thấp hơn ở các năng lực vận hành sâu,

Đánh giá khoảng cách giữa yêu cầu chính sách và năng lực an toàn thông tin  
 tại Hệ thống Quỹ tín dụng nhân dân Việt Nam

**Bảng 7. Điểm ATTT theo vùng địa lý**

Miền	n	Điểm TB TC4 (A)	SD	% dưới E=2.5	Detect (A)	Recover (A)	GAP (A - 2.5)
Miền Bắc	556	1,914	0,544	87,95%	0,732	1,111	-0,586
Miền Nam	210	1,878	0,628	86,67%	0,729	1,106	-0,622
Miền Trung	302	1,857	0,55	88,08%	0,73	0,996	-0,643

Nguồn: Kết quả xử lý số liệu khảo sát, 2025

đặc biệt tại Detect và Recover. Các nhóm quy mô lớn hơn có xu hướng tốt hơn; tuy nhiên, do cỡ mẫu của các nhóm từ 500 tỷ trở lên còn nhỏ, kết quả này chủ yếu được hiểu như tín hiệu mô tả hơn là bằng chứng suy luận về khác biệt giữa các nhóm.

Tổng hợp lại, kết quả mô tả cho thấy thiếu hụt ATTT xuất hiện khá đồng đều theo miền, trong khi theo quy mô có dấu hiệu phân tầng rõ hơn, với nhóm quy mô nhỏ là nhóm cần ưu tiên quan sát trong thảo luận chính sách. Đây là cơ sở thực chứng để phân sau phát triển lập luận về nguyên tắc tương xứng, theo đó các giải pháp hỗ trợ cần phù hợp hơn với khả năng nguồn lực và mức độ phức tạp vận hành của từng nhóm đơn vị.

## 5. Thảo luận và hàm ý chính sách

### 5.1. Thảo luận kết quả dưới lăng kính năng lực và áp lực thể chế

Kết quả ở Phần 4 chỉ ra sự mất cân đối rõ nét: lớp thiết lập/tuân thủ (đặc biệt là Nhận diện) đạt mức tương đối cao hơn, trong khi các năng lực vận hành sâu như Phát hiện

và Phục hồi lại thiếu hụt đáng kể. Sự chênh lệch này cho thấy thách thức lớn nhất không nằm ở sự hiện diện của quy trình, mà ở khả năng chuyển hóa chúng thành năng lực thực chất.

Dưới lăng kính thể chế, chênh lệch giữa Policy\_Score và Action\_Score phản ánh sự lệch pha giữa thiết lập và thực thi. Hệ thống có thể nhanh chóng hình thành các quy định chuẩn hóa để đáp ứng yêu cầu, nhưng lại chậm tích hợp vào vận hành do rào cản nguồn lực và kỷ luật thực thi. Tuy nhiên, do giới hạn của thiết kế cắt ngang, kết quả này chỉ được diễn giải như một chỉ dấu gợi ý cho “ngịch lý tuân thủ”, chưa đủ cơ sở để khẳng định trực tiếp cơ chế “tách rời” theo nghĩa đầy đủ.

Dưới lăng kính RBV, vùng trùng ở Phát hiện và Phục hồi- những khâu đòi hỏi chuyên môn sâu và phối hợp liên tục- phản ánh rõ giới hạn của nguồn lực nền tảng. Sự yếu kém rõ rệt của nhóm QTDND quy mô nhỏ (Mục 4.4) cho thấy nỗ lực đơn lẻ của từng quỹ khó có thể thu hẹp khoảng cách năng lực nếu thiếu cơ chế hỗ trợ ở cấp hệ thống.

**Bảng 8. Điểm ATTT và năng lực vận hành sâu theo nhóm quy mô (E = 2,5)**

Nhóm quy mô	n	Điểm TB TC4 (A)	% dưới E=2,5	Detect (A)	Recover (A)	GAP (A- 2,5)
< 100 tỷ	297	1,837	91,58%	0,65	0,978	-0,663
100- < 500 tỷ	744	1,901	87,33%	0,75	1,1	-0,599
500- < 1000 tỷ	20	2,098	65,00%	0,85	1,367	-0,402
> 1000 tỷ	7	2,344	57,14%	1,5	1,619	-0,156

Nguồn: Kết quả xử lý số liệu khảo sát, 2025

## 5.2. Hàm ý chính sách: từ “kiểm soát tuân thủ” sang “kiến tạo năng lực”

Chính sách quản lý cần tái cân bằng giữa yêu cầu tuân thủ và kiến tạo năng lực thực chất, tập trung vào các vùng thiếu hụt thuộc lớp Phát hiện- Ứng phó- Phục hồi. Khoảng cách lớn giữa thực tế và kỳ vọng cho thấy tuân thủ là nền tảng cần thiết nhưng chưa đủ. Để hỗ trợ các đơn vị hạn chế nguồn lực, hệ thống cần ưu tiên phát triển cơ chế “năng lực dùng chung”, trong đó một đầu mỗi tập trung cung cấp các dịch vụ giám sát và ứng cứu cốt lõi như phân tích nhật ký tập trung, cảnh báo tự động và điều phối theo kịch bản; qua đó bù đắp điểm yếu ở lớp Action, tối ưu chi phí bình quân và chuẩn hóa vận hành toàn hệ thống. Đồng thời, cần áp dụng nguyên tắc tương xứng theo quy mô: nhóm quy mô nhỏ nên ưu tiên bảo đảm kết nối và sử dụng hiệu quả năng lực dùng chung, trong khi nhóm lớn hơn cần từng bước nâng cao mức độ tự chủ và năng lực ứng cứu tại chỗ. Cuối cùng, điểm yếu ở Phục hồi cho thấy cần ưu tiên cách tiếp cận “học bằng thực hành”, thông qua diễn tập định kỳ và theo dõi các chỉ số vận hành như MTTD và MTTR, nhằm rút ngắn khoảng cách giữa hồ sơ tuân thủ và năng lực chống chịu thực tiễn.

## 6. Kết luận

Nghiên cứu đã đo lường khoảng cách giữa ngưỡng tối thiểu  $E = 2,5$  và năng lực an toàn thông tin thực tế của hệ thống QTDND Việt Nam trên cơ sở dữ liệu khảo sát diện

rộng năm 2025. Kết quả cho thấy năng lực an toàn thông tin trung bình của hệ thống còn dưới ngưỡng kỳ vọng, với tỷ lệ đơn vị chưa đạt chuẩn ở mức rất cao. Phân rã theo 5 chức năng NIST cho thấy thiếu hụt tập trung rõ nhất ở Phát hiện và Phục hồi, trong khi lớp Nhận diện/Bảo vệ đạt mức tương đối cao hơn.

Trên cơ sở đó, nghiên cứu cung cấp bằng chứng định lượng ở cấp hệ thống về khoảng cách giữa yêu cầu chính sách và năng lực thực thi, đồng thời gợi ý sự lệch pha giữa lớp thiết lập/tuân thủ và lớp thực thi vận hành. Hàm ý chính sách là cần tái cân bằng giữa tuân thủ và kiến tạo năng lực, theo hướng ưu tiên dịch vụ dùng chung, nguyên tắc tương xứng theo quy mô và chuẩn hóa hoạt động diễn tập- phục hồi ở cấp hệ thống. Nghiên cứu có một số hạn chế: Thứ nhất, do sử dụng dữ liệu cắt ngang, kết quả phù hợp để mô tả hiện trạng, xác lập đường cơ sở và chẩn đoán khoảng cách tại thời điểm khảo sát, nhưng không cho phép suy luận quan hệ nhân quả hay theo dõi sự hình thành khoảng cách theo thời gian. Thứ hai, dữ liệu dựa trên tự đánh giá ở cấp đơn vị nên có thể chịu ảnh hưởng của sai lệch khai báo hoặc xu hướng đánh giá lạc quan, nhất là ở các chỉ báo phản ánh tuân thủ hình thức. Vì vậy, kết quả nên được hiểu chủ yếu như bằng chứng chẩn đoán thực trạng ở cấp hệ thống, hơn là bằng chứng kiểm toán độc lập về hiệu năng vận hành. Các nghiên cứu tiếp theo nên kết hợp dữ liệu dọc, chỉ báo vận hành thực tế và/hoặc đánh giá độc lập để củng cố độ vững của kết luận. ■

## Tài liệu tham khảo

- Adejumo, A. P., & Ogburie, C. P. (2025). Strengthening finance with cybersecurity: Ensuring safer digital transactions. *World Journal of Advanced Research and Reviews*, 25(3), 1527–1541. <https://doi.org/10.30574/wjarr.2025.25.3.0908>
- Antunes, M., Maximiano, M., Gomes, R., & Pinto, D. (2021). Information security and cybersecurity management: A case study with SMEs in Portugal. *Journal of Cybersecurity and Privacy*, 1(2), 219–238. <https://doi.org/10.3390/jcp1020012>
- Barney, J. B. (1991). Firm resources and sustained competitive advantage. *Journal of Management*, 17(1), 99–120. <https://doi.org/10.1177/014920639101700108>
- Bộ Thông tin và Truyền thông. (2023). Quyết định số 2158/QĐ-BTTTT phê duyệt đề án xác định chỉ số đánh giá mức độ

Đánh giá khoảng cách giữa yêu cầu chính sách và năng lực an toàn thông tin  
tại Hệ thống Quỹ tín dụng nhân dân Việt Nam

- chuyển đổi số doanh nghiệp và hỗ trợ thúc đẩy doanh nghiệp chuyển đổi số, ban hành ngày 07 tháng 11 năm 2023. <https://thuvienphapluat.vn/van-ban/Doanh-nghiep/Quyết-dinh-2158-QĐ-BTTTT-2023-xac-dinh-Chi-so-danh-gia-muc-do-chuyen-doi-so-doanh-nghiep-585832.aspx>
- Brando, D., Kotidis, A., Kovner, A., Lee, M., & Schreft, S. L. (2022). Implications of Cyber Risk for Financial Stability. <https://www.federalreserve.gov/econres/notes/feds-notes/implications-of-cyber-risk-for-financial-stability-20220512.html>
- Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness. *MIS Quarterly*, 34(3), 523–548. <https://doi.org/10.2307/25750690>
- Cartwright, A., Cartwright, E., & Edun, E. S. (2023). Cascading information on best practice: Cyber security risk management in UK micro and small businesses and the role of IT companies. *Computers & Security*, 131, 103288. <https://doi.org/10.1016/j.cose.2023.103288>
- DiMaggio, P. J., & Powell, W. W. (1983). The iron cage revisited: Institutional isomorphism and collective rationality in organizational fields. *American Sociological Review*, 48(2), 147–160. <https://doi.org/10.2307/2095101>
- Gordon, L. A., Loeb, M. P., & Zhou, L. (2011). The impact of information security breaches: Has there been a downward shift in costs?. *Journal of Computer Security*, 19(1), 33–56. <https://doi.org/10.3233/JCS-2009-0398>
- Hsu, C., Lee, J.-N., & Straub, D. W. (2012). Institutional influences on information systems security innovations. *Information Systems Research*, 23(3-part-2), 918–939. <https://doi.org/10.1287/isre.1110.0393>
- Kshetri, N. (2013). Cybercrime and cybersecurity in the Global South. *Third World Quarterly*, 34(3), 411–427. <https://doi.org/10.1057/9781137021946>
- Lee, G., Kim, S., Lee, I., Brown, S., & Carbajal, Y. A. (2025). Adapting cybersecurity maturity models for resource-constrained settings: A case study of Peru. *The electronic journal of information systems in developing countries*, 91(1), e12350. <https://doi.org/10.1002/isd2.12350>
- Meyer, J. W., & Rowan, B. (1977). Institutionalized organizations: Formal structure as myth and ceremony. *American Journal of Sociology*, 83(2), 340–363. <https://doi.org/10.1086/226550>
- National Institute of Standards and Technology [NIST]. (2016). *Small business information security: The fundamentals* (NISTIR 7621 Rev. 1). U.S. Department of Commerce. <https://doi.org/10.6028/NIST.IR.7621r1>
- Ngân hàng Hợp tác xã Việt Nam. (2025). Báo cáo nội bộ. [Tài liệu nội bộ].
- Ngân hàng Nhà nước. (2021). *Quyết định số 810/QĐ-NHNN phê duyệt Kế hoạch chuyển đổi số ngành Ngân hàng đến năm 2025, định hướng đến năm 2030*, ban hành ngày 22 tháng 04 năm 2021. <https://thuvienphapluat.vn/van-ban/Tien-te-Ngan-hang/Quyết-dinh-810-QĐ-NHNN-2021-phe-duyet-Ke-hoach-Chuyen-doi-so-nganh-Ngan-hang-den-2025-474917.aspx>
- Nguyen, N. T., Hoang, T. H., Dinh, T. N. H., Szybowska, S., Nga, L., & Huong, L. (2020). Technology quality management of the industry 4.0 and cybersecurity risk management on current banking activities in emerging markets- The case in Vietnam. *International Journal for Quality Research*, 15, 845–856. <https://doi.org/10.24874/IJQR15.03-10>
- Opoku, D., Donkor, C., & Owusu-Bempah, E. (2025). Examining why hackers target banking systems: Lessons from the experiences of Ghanaian microfinance institutions. *DS Journal of Cyber Security*, 3(1), 24–33. <https://doi.org/10.59232/CYS-V3I1P102>
- Proença, D., & Borbinha, J. (2018, June). Information security management systems-a maturity model based on ISO/IEC 27001. In *International Conference on Business Information Systems* (pp. 102-114). Cham: Springer International Publishing.. [https://doi.org/10.1007/978-3-319-93931-5\\_8](https://doi.org/10.1007/978-3-319-93931-5_8)
- Rea-Guaman, A. M., San Feliu, T., Calvo-Manzano, J. A., & Sanchez-Garcia, I. D. (2017). Comparative study of cybersecurity capability maturity models. In *A. Mas, A. Mesquida, R. O'Connor, T. Rout, & A. Dorling (Eds.), Software Process Improvement and Capability Determination* (pp. 100–113). Springer. [https://doi.org/10.1007/978-3-319-67383-7\\_8](https://doi.org/10.1007/978-3-319-67383-7_8)
- Setia M. S. (2016). Methodology Series Module 3: Cross-sectional Studies. *Indian journal of dermatology*, 61(3), 261–264. <https://doi.org/10.4103/0019-5154.182410>
- Tam, L. T., Chau, N. M., Mai, P. N., Phuong, N. H., & Tran, V. K. H. (2020). Cyber crimes in the banking sector: Case study of Vietnam. *International Journal of Social Science and Economics Invention*, 6(05), 277–272- 277. <https://doi.org/10.23958/ijsssei/vol06-i05/207>
- Verizon. (2024). 2024 Data Breach Investigations Report. Verizon. <https://www.verizon.com/business/resources/T735/reports/2024-dbir-data-breach-investigations-report.pdf>