Nhận thức về gian lận và thông tin hữu ích cho khách hàng ANZ

Lời giới thiệu

Gian lận là một đối tác thầm lặng trong doanh nghiệp?

Nếu "gian lận" là một quốc gia, thì nền kinh tế của nó sẽ được xếp hạng thứ 5 trên thế giới – theo tiêu chuẩn đo lường gian lận của KPMG. Đáng lưu ý hơn đó là 80% các vụ vi phạm trong doanh nghiệp do nhân viên thực hiện. Nguyên nhân thường bắt nguồn từ việc lợi dụng sự yếu kém trong quản lý.

Mục đích của gói đào tạo này là nhằm nâng cao nhận thức và cung cấp những giải pháp hữu ích về việc nâng cao kiểm soát nội bộ và giảm bớt các thiệt hại có thể xảy ra do gian lận.

Là chủ doanh nghiệp hoặc nhà quản lý tài chính nên thận trọng cân nhắc về việc áp dụng các giải pháp này trong doanh nghiệp, hoặc các giải pháp thích hợp khác nhằm giảm thiểu các khả năng xảy ra gian lận.

Các khía cạnh được đề cập đến bao gồm

- Gian lận séc thanh toán
- Gian lận hoá đơn
- Lừa đảo trên mạng
- Đánh cắp thông tin nhận dạng
- Ăn cắp thông tin thẻ
- Đánh cắp email
- Điều khiển quyền truy cập
- Quản lý tài chính
- Các chính sách lao động

Gian lận séc thanh toán

Gian lận séc thanh toán vẫn là một trong những thách thức mà doanh nghiệp và các tổ chức tài chính phải đối mặt. Nó có thể được thực hiện bởi những người trong doanh nghiệp cũng như các tổ chức bên ngoài và có thể có nhiều cách thức, bao gồm:

- Hình thức bị thay đổi (bao gồm người nhận hoặc trị giá số tiền).
- Làm giả (chữ ký).
- Sao chép hoặc làm giả tờ séc.
- Hối phiếu giả (các tờ séc vô giá trị lưu thông tuần hoàn giữa các tài khoản với số tiền không rõ ràng).

Những lưu ý quan trọng giúp tránh việc gian lận séc thanh toán, gồm:

- Không ký lên tờ séc để trống.
- Chỉ ký lên tờ séc sau khi đảm bảo rằng các thông tin trên đó đã được điền đầy đủ.
- Các thông tin trên tờ séc cần phải đảm bảo không thể tuỳ ý sửa đổi để giảm nguy cơ gian lận, như: điền đầy đủ thông tin người nhận. Ví dụ, Sở thuế vụ Úc.
- Phải đảm bảo rằng nét chữ khi viết séc phải đậm nét, rõ ràng, nhất quán và không để quá nhiều khoảng trống giữa các từ và số. Viết từ trái sang phải.
- Giới hạn số lượng người có thẩm quyền ký séc.
- Thực hiện kiểm tra sổ sách theo định kỳ, ít nhất 12 tháng 1 lần .
- Nên có tối thiểu 2 người có thẩm quyền cùng ký lên tờ séc.
- Giữ lại một danh sách để ghi số seri của các loại séc đã nhận.
- Nếu tờ séc bị mất, đánh cắp hoặc thất lạc, ngay lập tức thông báo cho tổ chức tài chính và yêu cầu "Dừng chi trả" và/ hoặc huỷ tờ séc.
- Nếu là tờ séc tự in, cần phải đảm bảo các đặc điểm an toàn đã được tính đến để tránh việc giả mạo và sửa đổi trái phép.
- Cân đối các tờ séc với bản kê khai.
- Bảo mật séc và giới hạn quyền tiếp cận sổ séc.

Gian lận hoá đơn

Gian lận hoá đơn đang trở nên ngày càng phổ biến và, dù có thể được thực hiện bằng nhiều cách khác nhau, nhưng tóm lại nó xảy ra khi kẻ xấu lấy được các hoá đơn gốc hoặc thay đổi các chi tiết trên đó để gửi đến một tài khoản do họ quản lý. Thông thường, doanh nghiệp chỉ phát hiện ra họ là nạn nhân của các vụ gian lận hoá đơn khi nhà cung cấp liên lạc thông báo về việc chưa thanh toán đơn hàng.

Các vụ gian lận hoá đơn diễn ra theo các cách thức sau:

- Kẻ gian đóng giả là nhà cung cấp và liên hệ với doanh nghiệp, bằng điện thoại, emails hoặc fax để thông báo về việc thay đổi thông tin tài khoản.
- Hệ thống CNTT của doanh nghiệp bị hack hoặc bị ảnh hưởng bởi các phần mềm độc hại. Các thông tin tài khoản của nhà cung cấp bị thay đổi trong điều kiện Internet banking và khi doanh nghiệp thực hiện việc thanh toán cho nhà cung cấp, tiền sẽ được chuyển thẳng đến tài khoản của kẻ gian.
- Bưu phẩm của doanh nghiệp bị chặn lại và các thông tin tài khoản trên hoá đơn bị thay đổi, hoặc hoá đơn bị thay thế bằng một cái giả mạo.

Phát hiện gian lận hoá đơn

Gian lận hoá đơn được thực hiện dựa vào sự can thiệp và thay đổi thông tin thanh toán. Do đó, cách tốt nhất để phát hiện ra các vụ gian lận hoá đơn là dựa vào sự kết hợp của các đặc điểm sau:

- Kiểm tra về mặt hình thức các hoá đơn nhận được và so sánh nó với một hoá đơn gốc. Các hoá đơn đã bị chỉnh sửa/ làm giả có thể sử dụng các mực in, kiểu chữ, logo công ty khác với bản gốc hoặc bị mờ. Các thông tin liên lạc như số điện thoại, địa chỉ email cũng có thể bị thay đổi.
- Trong trường hợp thay đổi địa chỉ email, địa chỉ email bị đổi hầu như giống hệt, chỉ thay đổi tên miền một cách rất tinh vi (vd: ".org" thành ".com").

Các giải pháp làm giảm rủi ro của gian lận hoá đơn

- Thường xuyên cập nhật các phần mềm diệt virus để đảm bảo hệ thống máy tính của doanh nghiệp không bị ảnh hưởng bởi các phần mềm độc hại.
- Khi nhà cung cấp yêu cầu thay đổi thông tin, cần xác nhận thông tin đó với ngân hàng. Luôn sử dụng thông tin liên lạc của nhà cung cấp mà bạn lưu trữ trong hồ sơ, thay vì dựa vào các bức thư báo thay đổi thông tin liên lạc.
- Hướng dẫn nhân viên chú ý những điểm bất thường trên hóa đơn, đặc biệt là những thay đổi về đặc điểm và hình thức.
- Cần gửi thư xác nhận đến nhà cung cấp, thông báo đã thực hiện và các thông tin chi tiết của việc thanh toán.
- Khi sử dụng các thông tin mới hoặc sửa đổi, liên hệ với nhà cung cấp trước khi thực hiện thanh toán.

Lừa đảo trên mạng

Lừa đảo là một trong những phương thức đơn giản nhất, nhưng lại hiệu quả khi khiến nhiều người trở thành nạn nhân của nó. Mặc dù lừa đảo có nhiều hình thức khác nhau, nhìn chung, chúng trình diễn cho nạn nhân bằng một kịch bản "không tưởng". Nạn nhân hoặc sẽ được nhận một phần tiền lời rất nhỏ (số tiền có được do việc làm ăn phi pháp) hoặc nhận một phần tiền thưởng.

Những dấu hiệu cảnh báo khi bạn hoặc khách hàng của bạn là mục tiêu của các vụ lừa đảo.

- Bạn đã từng thắng 1 giải xổ số mà mình chưa hề tham gia?

- Bạn đã từng gặp 1 ai đó trên mạng và yêu cầu bạn gửi tiền cho họ để đầu tư hoặc giúp đỡ họ vượt qua những khó khăn cá nhân (họ đang gặp nguy hiểm, hoặc người thân bị ốm)? Họ cũng có thể sử dụng các lý do này nhờ bạn nhận tiền giúp.
- Bạn đã từng được mời tham gia vào một kế hoạch đầu tư đem lại lợi nhuận cao và rủi ro tương đối thấp?
- Bạn có khoản hoa hồng cho việc nhận các khoản tiền thông qua tài khoản ngân hàng hoặc PayPal?
- Bạn có đang nhận tiền mặt hoặc tờ séc khi tham gia chương trình 'Làm việc online tại nhà'?
- Bạn đã từng mua một món đồ trên mạng nhưng nó không bao giờ được chuyển đến?
- Bạn có bao giờ trả lời email yêu cầu bạn xác nhận, cập nhật hoặc cung cấp thông tin tài khoản ngân hàng?
- Bạn có được yêu cầu trả tiền để nhận phần thừa kế từ một người thân mà bạn không hề biết?
- Bạn từng bị buộc trả phí quá cao và được yêu cầu đóng một khoản tiền danh nghĩa để họ hoàn phí cho bạn?
- Bạn đã từng được nhờ chuyển tiền ra nước ngoài bằng Western Union, Money Gram hoặc các tổ chức dịch vụ tiền tệ (MSB)?

Nếu câu trả lời là "có" cho bất kỳ câu hỏi ở trên, bạn nên lập tức liên hệ với nhân viên đại diện ANZ.

Tài liệu tham khảo có sẵn

- anz.com
- Scamwatch.govt.au

Đánh cắp thông tin nhận dạng

Đánh cắp thông tin nhận dạng là một hình thức gian lận khi một người đạt được ích lợi về tài chính khi đóng giả một người khác. Để lấy được thông tin nhận dạng, kẻ gian cần có được các thông tin cá nhân. Họ có thể đánh cắp nó bằng nhiều phương thức khác nhau. Kẻ gian có thể sử dụng thông tin nhận dạng của bạn để lấy tiền tín dụng, tiếp cận tiền quỹ của bạn và thậm chí là để mở tài khoản ngân hàng.

Kẻ gian có được thông tin cá nhân của bằng các phương pháp sau:

- Đánh cắp email của bạn.
- Thông qua mã BINs để lấy các tài liệu mà bạn chưa tiêu huỷ hoàn toàn.
- Thông qua hình thức "Tấn công giả mạo[1]" (Phishing), ví dụ như một email hoặc tin nhắn yêu cầu cung cấp thông tin cá nhân hoặc tài khoản ngân hàng. Các email "Tấn công giả mạo" nhìn có vẻ giống như được gửi từ các nguồn hợp pháp, ví dụ như tổ chức tài chính.

Các giải pháp giúp ngăn chặn việc đánh cắp thông tin nhận dạng

- Bảo mật các dữ liệu cá nhân tại nhà hoặc nơi làm việc.
- Tiêu huỷ các tài liệu mà bạn vứt bỏ.
- Bảo mật hộp thư bằng khoá và phải cập nhật địa chỉ mới với các cơ quan, tổ chức khi bạn thay đổi chỗ ở.
- Phải đảm bảo rằng mã bảo vệ kiên cố và cập nhật các phần mềm diệt virus được cài đặt trong máy.
- Không cung cấp thông tin cá nhân hoặc tài khoản ngân hàng qua email.
- Không nhập thông tin cá nhân hoặc tài khoản ngân hàng vào một website nếu bạn không chắc về độ xác thực của nó.
- Truy cập trực tiếp vào website bằng cách gõ đường dẫn trong thanh công cụ, không nhấp vào bất kỳ đường dẫn nào có trong email.
- Kiểm tra sao kê tài khoản ngân hàng đều đặn, liên hệ với ngân hàng nếu không nhận ra bất cứ giao dịch nào.

[1] Email "tấn công giả mạo" có giao diện giống như được gửi từ nguồn hợp pháp và yêu cầu cung cấp các thông tin mật một cách bất hợp pháp.

Ăn cắp thông tin thẻ

Ăn cắp thông tin thẻ xảy ra khi kẻ gian thu thập một cách bất hợp pháp các dữ liệu trên dải từ của thẻ ghi nợ hoặc thẻ ghi có. Sau đó, chúng sử dụng các thông tin này để thực hiện các giao dịch phi pháp.

Các phương thức ăn cắp thông tin thẻ

- Một thiết bị dùng để ăn cắp thông tin có thể được lắp trên các máy ATM thực của ngân hàng để sao chép các dữ liệu trên thẻ khi khách hàng sử dụng thẻ tại ATM.
- Đối với các loại thẻ cho phép thực hiện việc chi trả không có mặt của thẻ (ví dụ như "Paywave" hoặc "Touch and Go"), kẻ gian có thể có được các thông tin chi tiết bằng thiết bị đọc thẻ di động. Thiết bị đọc thẻ di động cần nằm trong một khoảng cách nhất định với thẻ mà nó cần đọc.
- Máy chuyển tiền tự động thực tại các điểm bán hàng (ví dụ: EFTPOS) có thể bị thay thế bằng các thiết bị giả mạo để lấy dữ liệu thẻ và/ hoặc mã PIN.

Các giải pháp giúp làm giảm rủi ro ăn cắp thông tin thẻ.

- Thận trọng với bất kỳ máy ATM nào khả nghi. Lập tức báo với ngân hàng nếu có bất kỳ điểm bất thường nào, không thử di dời các thiết bị.
- Che mã PIN lại khi sử dụng ATM.
- Giữ thẻ cẩn thận trong một vật chứa an toàn mà thiết bị đọc thẻ di động không thể dò được (ví dụ như chiếc ví có lớp lót nhám).
- Xem thẻ như tiền mặt và luôn giữ thẻ bên mình. Nếu có thể, tránh đưa thẻ cho nhân viên cửa hàng hoặc người hầu bàn và để họ đem thẻ đi khuất tầm mắt bạn.
- Định kỳ kiểm tra sao kê ngân hàng và đảm bảo rằng bạn nhận ra tất cả các giao dịch. Nếu không, lập tức liên hệ với ANZ.

Ăn cắp email

Ăn cắp email xảy ra khi kẻ gian truy cập trái phép vào tài khoản email cá nhân hoặc của doanh nghiệp và sau đó gửi email từ tài khoản đó đến các tổ chức tài chính yêu cầu thực hiện các giao dịch khẩn cấp. Nó cũng được xem như là một loại đánh cắp thông tin nhận dạng điện tử.

Ăn cắp email có thể xảy ra khi

- Tài khoản email cá nhân/ doanh nghiệp có thể bị lộ do bị đánh cắp hoặc thông qua các email "Tấn công giả mạo". Do đó, cập nhật phần mềm diệt virus và thiết lập mật mã bảo vệ kiên cố rất quan trọng trong việc giảm thiểu rủi ro email bị đánh cắp.
- Kẻ gian có thể đóng giả là khách hàng và gửi email đến tổ chức tài chính, yêu cầu cung cấp một bảng cân đối tài khoản hoặc chuyển tiền điện tử quốc tế.
- Để tránh cuộc gọi xác nhận từ tổ chức tài chính, kẻ gian giả vờ như đang có cuộc họp hoặc đang trên đường đến dự đám tang và do đó sẽ không thể trả lời bất cứ cuộc gọi nào.

Làm thế nào để tránh việc đánh cắp email

- Bảo mật tài khoản email: Không cung cấp địa chỉ email và password cho bất cứ ai.
- Thay đổi password ngay lập tức nếu bạn nghi ngờ nó đã bị lộ.
- Thay đổi password thường xuyên và nên sử dụng password kiên cố và khó có thể đoán ra.
- Duy trì việc cập nhật các phần mềm bảo mật.
- Theo quan điểm nghiệp vụ, luôn thực hiện các quy trình gọi xác nhận đến khách hàng và nhà cung cấp khi nhận được email yêu cầu thực hiện giao dịch.

Làm thế nào để phát hiện email bị ăn cắp

Nếu khách hàng hoặc nhà cung cấp của bạn trở thành nạn nhân của việc ăn cắp email, bạn có thể sẽ nhận một yêu cầu chuyển tiền điện tử quốc tế (ITT) khẩn cấp. Bạn cũng có thể nhận ra:

- Sự thay đổi trong cách trả lời mail của khách hàng (Ví dụ như sai ngữ pháp hoặc từ vựng).
- Từ chối trả lời cuộc gọi xác nhận

Các phương thức chủ động phòng ngừa nói chung

Kiểm soát quyền truy cập

Những nhân viên lợi dụng sự yếu kém trong việc quản lý truy cập thường phải chịu trách nhiệm nếu gian lận nội bộ xảy ra. Do đó, việc quản lý thích hợp, ví dụ như hạn chế việc truy cập hệ thống, chỉ cho phép khi cần biết những thông tin cơ bản và giới hạn quyền truy cập vào các tài liệu nhạy cảm, là phương thức chủ động ngăn chặn việc gian lận.

Các bước cơ bản để nâng cao việc kiểm soát truy cập trong doanh nghiệp

- Thực hiện chính sách quy định rằng tất cả các tài liệu mật, tờ séc và sao kê ngân hàng phải được cất giữ cẩn thận khi không dùng đến.
- Chỉ cung cấp thông tin và tài liệu khi cần.
- Hạn chế quyền truy cập vào thông tin tài khoản ngân hàng, hình thức thanh toán (ví dụ như tờ séc) và phương thức thanh toán (ví dụ internet banking). Định kỳ kiểm tra lại những nhân viên được truy cập vào các thông tin này và huỷ quyền truy cập đối với các nhân viên không còn nhu cầu sử dụng thông tin.
- Khi một nhân viên rời khỏi công ty, phải đảm bảo rằng tất cả các trang thiết bị cần thiết (vd: laptop, điện thoại, …) được hoàn trả lại. Thẻ ra vào văn phòng, quyền truy cập tất cả các hệ thống ngay lập tức được thu hồi.
- Thay đổi tất cả các password của hệ thống thanh toán mà họ có thể đã được truy cập.
- Khuyến khích nhân viên thường xuyên thay đổi passwords.

Quản trị tài chính

Thực hiện tốt việc quản lý tài chính có thể giúp ngăn ngừa gian lận trong doanh nghiệp. Theo nghĩa đơn giản nhất, quản trị tài chính đề cập đến hệ thống phân quyền trong doanh nghiệp để đảm bảo quy trình hoạt động một cách hiệu quả.

Lưu ý

- Chỉ đạo việc kiểm toán định kỳ các báo cáo tài chính và hàng tồn kho.
- Định kỳ cân đối lại các báo cáo tài chính.
- Cân nhắc việc quản lý các khoản tiền không rõ nguồn gốc trong các cơ sở kinh doanh có liên quan đến việc giao dịch tiền mặt.
- Đảm bảo có sự phân công trách nhiệm trong doanh nghiệp, ví dụ một nhân viên không thể vừa nhận hoá đơn vừa chấp thuận việc thanh toán.

Các chính sách lao động

Nhân viên có thể là tài sản quý giá nhất hoặc rủi ro lớn nhất của doanh nghiệp nếu họ có cơ hội thực hiện các hành vi gian lận.

Lưu ý

- Phát triển Hệ thống tiêu chuẩn đạo đức để tất cả nhân viên tuân theo.
- Thiết lập tiêu chuẩn tối thiểu của đạo đức và hành vi.
- Triển khai các quy trình kiểm tra lý lịch nhân viên hiệu quả, bao gồm kiểm tra thông tin tham khảo thích hợp, lý lịch tư pháp và trình độ chuyên môn.

- Thực hiện các quy định nghỉ phép tối thiểu – nhiều trường hợp gian lận nội bộ xảy ra khi nhân viên có liên quan đang trong thời gian nghỉ phép; do đó nên cảnh giác với các nhân viên đang còn trong thời hạn nghỉ phép.
- Cần cảnh giác với việc chi tiêu bất thường hoặc sự thay đổi hành vi của nhân viên; xe hơi mới, quần áo đắt tiền, đi du lịch…
- Khuyến khích nhân viên nêu lên mối lo ngại về các hành vi không trung thực của nhân viên khác mà có thể ảnh hưởng đến doanh nghiệp.
- Đảm bảo rằng ban quản lý được trao quyền quản lý rủi ro gian lận và sai phạm.
- Giải thích cho cơ quan công an về quy định của tất cả sự việc gian lận nội bộ có liên quan để tiến hành việc khởi tố, bất kể các ảnh hưởng tài chính.

Các kế hoạc quản lý gian lận

ANZ đặc biệt khuyến khích việc thực hiện kế hoạch quản lý gian lận một cách hiệu quả - bạn hiểu rõ doanh nghiệp của bạn hơn bất cứ ai và sẽ nhận ra các rủi ro gian lận chủ yếu xuất phát từ đâu. Điều này giúp cho doanh nghiệp của bạn hoạt động có hiệu quả hơn và giúp tránh các thiệt hại có thể xảy ra do gian lận.

Tài liệu tham khảo có sẵn

- Australian Standards 8001-2008 Corruption & Control guide – www.standards.org.au
- Ernst & Young 12th global fraud survey 2011
- Deloitte Bribery & Corruption survey 2012
- KPMG Fraud barometer 2012

Để có thêm thông tin chi tiết

Tra cứu "Group Investigations" trên Max để tìm thông tin liên lạc tại địa phương.

Điều mục quản lý gian lận

Kế hoạch và nguồn lực

	✓
Bạn có các tài liệu chính thức về cách thức giải quyết hành vi gian lận và đã truyền đạt cho tất cả nhân viên?	
Các quy định/ quy trình xử lý gian lận và cách mà hành vi gian lận ngày càng leo thang được trình bày rõ ràng và dễ hiểu?	
Quá trình chi tiết đánh giá các rủi ro do gian lận đã được thực hiện?	
Trong sổ sách hoặc kế hoạch qủan lý rủi ro có dẫn chứng các rủi ro đã nhận diện được?	
Một kế hoạch xem xét các rủi ro do gian lận được thực hiện định kỳ?	
Nếu rủi ro đã được nhận diện, bạn có đánh giá chi phí phải chịu do các rủi ro gây ra?	
Đối với các rủi ro đã được xác định, bạn có nhận diện được ngưỡng kiềm chế tối đa dẫn đến hành vi gian lận?	
Bạn có bộ phận chịu trách nhiệm quản lý rủi ro gian lận; một "chuyên gia phòng chống gian lận" hoặc "người đại diện phòng chống gian lận"?	

Ngăn ngừa

	✓
Doanh nghiệp có xây dựng văn hoá khuyến khích và khen thưởng cho các hành vi đạo đức?	
Tất cả nhân viên hiểu về quy trình tố cáo gian lận và trách nhiệm của mỗi cá nhân?	
Quyền truy cập hệ thống của nhân viên được xem xét lại định kỳ để đảm bảo nhân viên chỉ có thể tiếp cận các chức năng cần thiết trong hệ thống để hoàn thành công việc?	
Các mật khẩu và mức độ tiếp cận hệ thống thanh toán và ngân hàng được xem xét lại và thay đổi định kỳ?	
Các quy trình và nhiệm vụ quan trọng được kiểm tra lại định kỳ để đảm bảo có sự phân quyền hợp lý?	
Hồ sơ lưu lại việc ra vào văn phòng được kiểm tra lại định kỳ để đảm bảo rằng việc ra vào của nhân viên bình thường và hợp lý?	
Các phương pháp bảo vệ các công cụ chuyển đổi và tài sản (vd: sổ séc, thể thức vay kinh doanh, tiền mặt, thẻ taxi, tài sản vật chất như: máy vi tính và hoặc công cụ dụng cụ)?	

Ngăn ngừa	✓
Doanh nghiệp định kỳ kiểm kê tài sản? (vd như laptop, điện thoại cố định, điện thoại Blackberry…)	
Doanh nghiệp giám sát những nhân viên nghỉ phép hằng năm quá nhiều? Doanh nghiệp có thực hiện các chính sách thích hợp quy định về nghỉ phép hằng năm?	
Doanh nghiệp quản lý và và phê chuẩn kế hoạch khuyến khích các nhân viên có thành tích cao trong công việc?	
Doanh nghiệp thực hiện quy trình kiểm tra lý lịch trước khi tuyển dụng? (vd: công việc trước đây, kiểm tra lý lịch tư pháp, kiểm tra các thông tin tham khảo)	
Có thực hiện các bước xem xét lại một cách độc lập các nhà cung cấp, khách hàng mới và hiện tại?	
Tất cả nhân viên đã hoàn thành khoá đào tạo nhận biết gian lận?	

Phát hiện	✓
Nhân viên có thể ẩn danh báo cáo mối nghi ngờ?	
Có quy trình phù hợp để công việc điều tra tiền hành thuận lợi?	
Cách tiếp cận nhân viên liên quan đến gian lận có phù hợp? Ví dụ như nhân viên biết rằng tất cả các vấn đề gian lận, kể cả tài sản, đều phải được báo cho cơ quan công an để tiến hành khởi tố.	
Doanh nghiệp có thực hiện việc kiểm tra sổ sách bất thường bên cạnh việc kiểm tra thường xuyên (cân đối tiền mặt và hàng tồn kho)?	
Sử dụng phần mềm máy tính để phát hiện hành vi gian lận?	

Phản ứng	✓
Khi hành vi gian lận bị phát hiện, doanh nghiệp có các thủ tục hoặc nguồn lực để xử lý?	
Thủ tục báo cáo các cơ quan có thẩm quyền về hành vi được xác định là gian lận có chặt chẽ?	
Doanh nghiệp có quy trình thu hồi lại tài sản hoặc tiền bị mất cắp?	
Doanh nghiệp có bảo hiểm cho các tổn thất xảy ra do gian lận?	

Phản ứng	✓
Doanh nghiệp có thường xuyên xem xét lại và theo dấu các tổn thất do gian lận và trường hợp bị thất thoát để tìm ra lỗ hổng trong việc quản lý cần lưu ý?	
Các vụ gây ra thất thoát lớn được xem xét lại để lưu ý đến việc phân tích quy trình/ kết quả và để giảm bớt thiệt hại một cách thích hợp?	
Các tổn thất do gian lận thường được báo cho cấp lãnh đạo?	
Doanh nghiệp có cập nhật các xu hướng gian lận và tổn thất bên ngoài để đảm bảo việc quản lý các mối đe doạ có thể xảy ra?	
Doanh nghiệp có báo cáo một cách chính xác và kịp lúc các trường hợp cố ý gian lận, hối lộ và tham nhũng, kể cả chưa xảy ra tổn thất cho giám đốc, ban quản lý, điều hành như yêu cầu?	
Các sản phẩm và/ hoặc nguồn đã được các chuyên gia phòng chống gian lận xem xét lại trước khi thông báo triển khai, nhằm đảm bảo sẽ làm giảm các rủi ro gian lận then chốt?	