To: Lớp NT207.P21.ANTT - CHUẨN BỊ KTGK và KTCK

BÀI TẬP môn QLRR & ATTT tại doanh nghiệp

TRẮC NGHIỆM (30 câu) & TỰ LUẬN (10 câu)

THỜI GIAN LÀM BÀI: 60 phút (1,5 phút/câu)

	Câu số 01	Câu số 02	Câu số 03	Câu số 04	Câu số 05	Câu số 06	Câu số 07	Câu số 08	Câu số 09	Câu số 10	Câu số 11	Câu số 12	Câu số 13	Câu số 14	Câu số 15	Câu số 16	Câu số 17	Câu số 18	Câu số 19	Câu số 20	Câu số 21	Câu số 22	Câu số 23	Câu số 24	Câu số 25	Câu số 26	Câu số 27	Câu số 28	Câu số 29	Câu số 30
a																														
b																														
c																														
d																														
e																														
f																														
g																														

A. PHẦN TRẮC NGHIỆM (30 câu)

1. Tiêu chuẩn ISO 27001:2013 yêu cầu các doanh nghiệp phải biên soạn và ban hành chính sách ATTT ("Information Security Policy") phù hợp với đặc điểm, chức năng và bối cảnh hoạt động của doanh nghiệp.

Theo bạn, doanh nghiệp gặp phải thách thức gì sau khi ban hành chính sách ATTT theo yêu cầu tại Nhóm A.5 Yêu cầu A.5.1 Điều A.5.1.1 theo Phụ lục A tiêu chuẩn ISO 27001:2013 - *chọn một câu trả lời (a/b/c/d/e/f) dưới đây làm đáp án của bạn cho câu hỏi này*:

a) Người lao động của doanh nghiệp không tuân thủ;
b) Sự mất lòng tin của nhân viên vào chính sách ATTT;
c) Người lao động của doanh nghiệp thiếu nhận thức về ATTT;
d) Lãnh đạo doanh nghiệp có cảm giác đã an toàn sau khi ban hành chính sách ATTT; và không hoặc quên cập nhật / nâng cấp hệ thống bảo mật thông tin tại doanh nghiệp;
e) Chọn tất cả a, b, c và d;
f) Chọn a, b và c.

2. Người kiểm tra ATTT tại doanh nghiệp đã kiểm tra chương trình chống vi-rút trên các máy chủ được lấy mẫu và máy trạm và nhận thấy rằng một số trong số chúng không có định nghĩa (hay không được cập nhật bản vá lỗi) chống vi-rút mới nhất.

Theo bạn, doanh nghiệp đã không đáp ứng (hay không phù hợp với) yêu cầu nào trong 14 yêu cầu và biện pháp kiểm soát phải có tại Nhóm A.12 của Phụ lục A - ISO 27001:2013- *chọn một câu trả lời (a/b/c/d) dưới đây làm đáp án của bạn cho câu hỏi này*:

a) A.12.2.1	b) A.12.5.1	c) A.12.6.1	d) A.12.6.2

3. Người kiểm tra ATTT tại doanh nghiệp quan sát và thấy rằng doanh nghiệp trang bị nhiều máy in cấp doanh nghiệp với các nhãn hiệu khác nhau từ các nhà sản xuất máy in khác nhau như HP ("Hewlett-Packard"), Canon, Epson, v.v. Khi tìm hiểu về hồ sơ mời thầu mua sắm các máy in này vào thời gian trước đây, bộ phận mua sắm tài sản CNTT của doanh nghiệp báo là việc mua sắm dựa vào sự phổ biến của nhãn hiệu, giá bán và các mối quan hệ giữa doanh nghiệp và đơn vị bán hàng. Hồ sơ mua sắm không có ghi chép gì về yêu cầu ATTT đối với các máy in này.

Theo bạn, doanh nghiệp đã không đáp ứng (hay không phù hợp với) 14 yêu cầu và biện pháp kiểm soát ("Control") nào tại Nhóm A.12 của Phụ lục A - ISO 27001:2013 - *chọn một câu trả lời (a/b/c/d/e/f) dưới đây làm đáp án của bạn cho câu hỏi này*:

a) A.12.2.1	b) A.12.5.1	c) A.12.6.1
d) A.12.2.1 và A.12.6.1	e) A.12.1.1 và A.12.2.1	f) Mua sắm máy in không liên quan đến Nhóm A.12

4. Người kiểm tra ATTT tại doanh nghiệp quan sát và thấy rằng không phải tất cả các thiết bị đều được kích hoạt cho ghi nhật ký (logging) và các thiết bị đã bật ghi nhật ký lại không ghi tất cả các hoạt động theo yêu cầu của ISO 27001:2013. Theo bạn, doanh nghiệp đã không đáp ứng (hay không phù hợp với) biện pháp kiểm soát ("Control") nào trong 14 biện pháp kiểm soát tại Nhóm A.12 của Phụ lục A - ISO 27001:2013 - *chọn một câu trả lời (a/b/c/d) dưới đây làm đáp án của bạn cho câu hỏi này*:

a) A.12.1.1 và A.12.1.2	b) A.12.4.1 và A.12.4.3	c) A.12.4.2, A.12.4.3 và A.12.4.4	d) A.12.6.1 và A.12.6.2

5. Theo dõi tin tức trên mạng, báo The Guardian (nước Anh) có đưa tin như sau về nguyên nhân khiến mạng xã hội Facebook gặp sự cố ngừng hoạt động hơn 5 giờ ngày 05/03/2024: *"Why did Facebook go down? Just before 5pm UTC, people began noticing they could not access Facebook, Instagram, WhatsApp or Messenger. It would be more than five hours before services would begin to be restored. Facebook issued a statement on Tuesday confirming that the cause of the outage was* ***a configuration change to the backbone routers*** *that coordinate network traffic between the company's data centres, which had a cascading effect, bringing all Facebook services to a halt. It meant not only was Facebook gone, but everything Facebook runs disappeared too.".*

Theo bạn, nếu dựa vào tin tức về sự cố mà Facebook gặp phải như trên, Facebook có thể đã không đáp ứng các yêu cầu ATTT nào trong Phụ lục A – ISO 27001:2013 - ***chọn một hay nhiều hơn*** *câu trả lời (a/b/c) dưới đây làm đáp án của bạn cho câu hỏi này*:

a) Nhóm A.17 Yêu cầu A.17.1 Điều A.17.1.1; Nhóm A.14 Yêu cầu A.14.2 Điều A.14.2.2;
b) Nhóm A.17 Yêu cầu A.17.1 Điều A.17.1.2; Nhóm A.12 Yêu cầu A.12.1 Điều A.12.1.2;
c) Nhóm A.17 Yêu cầu A.17.2 Điều A.17.2.1; Nhóm A.18 Yêu cầu A.18.2 Điều A.18.2.2;
d) Ý kiến khác: ……

6. Facebook gặp sự cố ngừng hoạt động trên toàn cầu vào ngày 5 tháng 3 năm 2024 trong hơn 5 giờ. Theo trang báo lỗi Downdetector, Facebook đã gặp sự cố nặng với hơn 81% số lượt tài khoản báo lỗi. Trang này ghi nhận khoảng 40.000 lượt báo lỗi trên Facebook và Instagram chỉ trong vòng 1 giờ.

Theo bạn, với thời gian gián đoạn dịch vụ như trên, nếu doanh nghiệp có ký hợp đồng dịch vụ với Facebook thì Facebook sẽ gặp rủi ro gì sau đây - *chọn một câu trả lời (a/b/c/d/e/f) dưới đây làm đáp án của bạn cho câu hỏi này*:

a) Bị phạt tiền vì vi phạm điều khoản về thỏa thuận mức độ dịch vụ ("Service Level Agreement" (SLA)) mà Facebook cung cấp cho khách hàng theo Nhóm A.15 Yêu cầu A.15.2 Điều A.15.2.2 Phụ lục A – ISO 27001:2013;
b) Mất khách hàng sau sự cố vì nhiều doanh nghiệp sẽ chuyển hoạt động qua mạng xã hội khác như dự phòng;
c) Từ bỏ sử dụng dịch vụ của Facebook;
d) Bị yêu cầu kiểm toán và có thể bị kiện do không tuân thủ các cam kết ATTT với khách hàng;
e) Chọn a, b, c và d;
f) Rủi ro khác. Nếu bạn chọn f thì bạn phải nêu ra Facebook sẽ gặp rủi ro gì khác với 4 rủi ro đã nêu ra ……
……

……

7. BYOD là viết tắt của "Bring Your Own Device" (Mang theo thiết bị của riêng bạn), đề cập đến xu hướng nhân viên sử dụng thiết bị cá nhân của riêng họ (ví dụ: điện thoại thông minh, máy tính xách tay, máy tính bảng, ổ USB, v.v.) để kết nối với mạng và hệ thống thông tin của doanh nghiệp hoặc tổ chức nơi họ làm việc. Để đáp ứng các yêu cầu ATTT tại Nhóm A.6 Yêu cầu A.6.2 Điều A.6.2.1 theo Phụ lục A – ISO 27001:2013 doanh nghiệp phải thiết lập biện pháp kiểm soát "*A policy and supporting security measures shall be adopted to manage the risks introduced by using mobile devices.*".

Theo bạn, rủi ro phát sinh khi dùng thiết bị di động ("mobile devices") là những rủi ro gì sau đây - *chọn một câu trả lời (a/b/c/d/e) dưới đây làm đáp án của bạn cho câu hỏi này*:

a) Thiếu sự theo dõi và giám sát của người phụ trách CNTT tại doanh nghiệp;
b) Rò rỉ dữ liệu, liên quan đến việc nhân viên sử dụng sai thông tin hoặc do bị trộm thiết bị;
c) Lây nhiễm phần mềm độc hại do thiếu kiểm soát các ứng dụng cài đặt trên thiết bị di động;
d) Vi phạm các yêu cầu tuân thủ luật và quy định về quyền riêng tư tại Điều 21 Hiến pháp 2013 của VN;
e) Chọn a, b, c và d. Nếu chọn e, bạn phải nêu ra thêm một rủi ro mà bạn biết khác với 4 rủi ro đã nêu ……

---

8. Trang mạng https://www.brusselstimes.com/ đưa tin ngày 15/03/2024 về Vương quốc Bỉ là các bộ trưởng, quan chức hàng đầu và các nhà ngoại giao của nước này sẽ nhận được điện thoại thông minh và máy tính xách tay bảo mật mới để ngăn chặn việc "hack" và nghe lén thông tin hoặc chặn liên lạc từ bên ngoài *"prevent external hacking and eavesdropping or communication being intercepted"*. Trích dẫn nội dung nguyên văn: *"Belgium launched a brand new communication system for those in government, as well as top officials, diplomats and crucial security functions. The closed system technology was developed entirely in Belgium with proprietary components, by the new entity Belgian Secure Communications (BSC), under the Justice Minister Paul Van Tigchelt. It will replace the BINII (Belgian Intelligence Network Information Infrastructure) – a secure communication platform set up in 2007 that allowed the sharing of sensitive and classified information. It is now outdated and no longer adapted to new technology and threats. Van Tigchelt highlighted an economic mission to China in 2019, in which 135 hacking attempts per hour were detected on the mobile phones of delegation members."*.

Bạn hãy cho biết hành động của Vương quốc Bỉ phù hợp với yêu cầu và mục tiêu nào trong Phụ lục A – ISO 27001:2013 - *chọn một câu trả lời (a/b/c/d/e/f) dưới đây làm đáp án của bạn cho câu hỏi này*:

a) Nhóm A.11 Yêu cầu A.11.2 Điều A.11.2.6	c) Nhóm A.12 Yêu cầu A.12.6 Điều A.12.6.1
b) Nhóm A.12 Yêu cầu A.12.6 Điều A.12.6.2	d) Nhóm A.13 Yêu cầu A.13.2 Điều A.13.2.1
e) Chọn a, b, c và d;	f) Chọn a, c và d

9. Trong thời đại kỹ thuật số, truy cập internet là nền tảng của xã hội hiện đại, tạo điều kiện thuận lợi cho giao tiếp, giáo dục và thương mại. Tuy nhiên, năm 2023 chứng kiến một xu hướng đáng lo ngại về việc ngừng hoạt động Internet tối đa (kéo dài nửa năm đến cả năm) ở 8 quốc gia khác nhau; mỗi quốc gia có bối cảnh riêng nhưng có chung một chủ đề chung là kiểm soát của chính phủ đối với luồng thông tin. Những lần ngừng hoạt động Internet không chỉ làm nổi bật sự cân bằng mong manh giữa quyền hưởng thụ dịch vụ kỹ thuật số mà còn có tác động kinh tế sâu sắc và làm gián đoạn cuộc sống hàng ngày của hàng triệu người.

Thông qua kiến thức, các mối quan hệ xã hội và mức độ hiểu biết về nhu cầu sử dụng Internet của bạn, theo bạn, lý do của việc các chính phủ một số nước cho ngừng tối đa hoạt động Internet là lý do gì sau đây - *chọn một câu trả lời (a/b/c/d/e/f) dưới đây làm đáp án của bạn cho câu hỏi này*:

a) Để duy trì trật tự công cộng trong bối cảnh căng thẳng sắc tộc tại một số nước;
b) Để tiết kiệm ngân sách đầu tư hệ thống (phần cứng, phần mềm, ứng dụng….) cung cấp dịch vụ trên Internet;
c) Để kiểm soát và hạn chế sự lan truyền thông tin trong trong thời điểm nhạy cảm;
d) Để bảo trì định kỳ hệ thống (phần cứng, phần mềm, ứng dụng….) cung cấp dịch vụ trên Internet;
e) Chọn a, b, c và d.
f) Chọn a và c.

10. Dịch địa chỉ mạng ("Network Address Translation") hay "NAT" là một quá trình trong đó một hoặc nhiều địa chỉ IP cục bộ ("local IP") được dịch thành một hoặc nhiều địa chỉ IP toàn cầu ("global IP") và ngược lại để cung cấp quyền truy cập Internet cho các máy chủ cục bộ. Ngoài ra, nó còn dịch số cổng, tức là che số cổng của máy chủ bằng một số cổng khác, trong gói sẽ được định tuyến đến đích. NAT tạo các mục địa chỉ IP - số cổng trong bảng NAT. NAT thường hoạt động trên bộ định tuyến hoặc tường lửa. Lợi ích của NAT là sử dụng lại địa chỉ IP riêng, tăng cường bảo mật cho các mạng riêng bằng cách giữ (hay che dấu) địa chỉ nội bộ ở chế độ riêng tư với mạng bên ngoài và sử dụng số lượng địa chỉ IP công cộng (bên ngoài) ít hơn, giúp bảo toàn không gian địa chỉ IP.

Bên cạnh những lợi ích của NAT thì xét về khía cạnh ATTT, sử dụng NAT cũng mang đến những vấn đề hay rủi ro về bảo mật. Theo bạn, rủi ro nào sau đây ảnh hưởng đến thuộc tính "Integrity" và "Availability" của thông tin - *chọn một câu trả lời (a/b/c/d/e/f) dưới đây làm đáp án của bạn cho câu hỏi này*:

a) Việc dịch địa chỉ gây ra độ trễ ("latency"), lỗi ("error") hoặc mất gói tin trên mạng ("packet loss");

b) Hạn chế khả năng kết nối của một số thiết bị và ứng dụng vì NAT có thể không hỗ trợ tất cả các giao thức hoặc không cho phép một số loại kết nối nhất định; chặn giao tiếp trực tiếp giữa các thiết bị ở sau thiết bị NAT;

c) Làm phức tạp thêm các giao thức đường hầm ("tunneling protocol") như IPsec, OpenVPN, PPTP, SSTP;

d) Cấu hình sai, ánh xạ ("mapping") địa chỉ IP thủ công hoặc không cập nhật NAT định kỳ;

e) Chọn a và b;

f) Chọn a, b, c và d.

11. Người kiểm tra ATTT tại doanh nghiệp quan sát và biết rằng bộ phận phụ trách mạng của doanh nghiệp đã triển khai kỹ thuật ảo hóa VLAN ("virtual local area network") cho mạng nội bộ của doanh nghiệp. VLAN (mạng cục bộ ảo) là một nhóm con của mạng, kết hợp nhiều thiết bị mạng thành một nhóm hoặc một miền và phân chia nó khỏi phần còn lại; hoặc nói một cách dễ hiểu thì VLAN chia một "*switch" thành nhiều "switch"* hoàn toàn độc lập với nhau. Tuy nhiên, khi Người kiểm tra ATTT muốn tham khảo tài liệu cấu hình VLAN thì người phụ trách bộ phận này đã từ chối với lý do bảo mật.

Theo bạn, nếu từ chối hoặc không cho kiểm toán bảo mật bởi một bên thứ ba (như Người kiểm tra ATTT được nêu trên) đối với VLAN thì doanh không đáp ứng với yêu cầu nào trong Phụ lục A – ISO 27001:2013 và các điểm yếu nào của VLAN có thể gây rủi ro cho mạng doanh nghiệp - *chọn một câu trả lời (a/b/c/d/e/f) dưới đây làm đáp án của bạn cho câu hỏi này:*

a) Nhóm A.12 Yêu cầu A.12.7 Điều A.12.7.1; cấu hình VLAN không đáp ứng theo tiêu chuẩn hoặc không theo thông lệ cấu hình tốt nhất *(*như có lỗi do *"misconfigured ports or insecure trunk links or insecure native VLAN or all VLAN traffic is routed through a single device,…")*;

b) Nhóm A.18 Yêu cầu A.18.2 Điều A.18.2.1, A.18.2.2 và A.18.2.3; không đánh giá và cập nhật bảo mật thường xuyên để xác định và giải quyết các lỗ hổng tiềm ẩn trong quá trình triển khai VLAN;

c) Thực thi kiểm soát truy cập yếu kém (AC);

d) Việc xử lý "VLAN tags" của các thiết bị mạng không phù hợp;

e) Chọn a và b;

f) Chọn a, b, c và d.

12. APT ("Advanced Persistent Threat (APT)") được nhiều tài liệu dịch là "Mối đe dọa dai dẳng nâng cao" cũng là kẻ tấn công dai dẳng, giấu mặt, âm thầm đánh cắp dữ liệu quan trọng trên hệ thống của mục tiêu. APT được tổ chức NIST https://csrc.nist.gov/glossary/term/advanced_persistent_threats định nghĩa như sau: *"An adversary with sophisticated levels of expertise and significant resources, allowing it through the use of multiple different attack vectors (e.g., cyber, physical, and deception) to generate opportunities to achieve its objectives, which are typically to establish and extend footholds within the information technology infrastructure of organizations for purposes of continually exfiltrating information and/or to undermine or impede critical aspects of a mission, program, or organization, or place itself in a position to do so in the future; moreover, the advanced persistent threat pursues its objectives repeatedly over an extended period of time, adapting to a defender's efforts to resist it, and with determination to maintain the level of interaction needed to execute its objectives."*

Theo bạn, APT có thể gây ra rủi ro gì cho tổ chức và/hoặc doanh nghiệp - *chọn một câu trả lời (a/b/c/d/e) dưới đây làm đáp án của bạn cho câu hỏi này:*

a) Xâm nhập, theo dõi, chặn tin, phá hại ngầm và đánh cắp dữ liệu nhạy cảm;

b) Làm ngừng hoạt động mạng ("Network Outage");

c) Từ chối dịch vụ (“Denial of Service – (DOS)”);
d) Lây nhiễm phần mềm độc hại vào hệ thống (“Infect systems with malware”);
e) Chọn a, b, c và d. Nếu chọn d, bạn phải nêu ra ít nhất tên một cuộc tấn công APT đã xảy ra ……..
……

13. Con người nói chung rất yếu kém trong việc phát hiện thông tin giả (“fake news or misinformation or disinformation”). Điều này là do tin giả thường trông giống tin thật. Một khi thông tin sai lệch đã có chỗ đứng thì rất khó sửa chữa. Rủi ro ở đây là những nỗ lực sửa chữa hay bác bỏ tin giả thường củng cố thêm niềm tin của công chúng vào nó (tin giả). Có 4 chiến lược quản lý rủi ro: Tránh rủi ro (“Risk Avoidance”), Giảm rủi ro (“Risk Mitigation”), Chuyển rủi ro (“Risk Transfer”) và Chấp nhận rủi ro (“Risk Acceptance or Risk Retention”) mà các doanh nghiệp và tổ chức phải chọn lựa và áp dụng để kiểm soát điểm yếu của người lao động (làm việc tại doanh nghiệp) như là điểm yếu kỹ thuật theo yêu cầu tại Nhóm A.12 Yêu cầu A.12.6 Điều A.12.6.1 theo Phụ lục A – ISO 27001:2013.

Theo bạn, để phòng chống rủi ro từ tin giả, các chiến lược nào sau đây thuộc chiến lược Tránh rủi ro (“Risk Avoidance”) bị tin giả thao túng - *chọn một câu trả lời (a/b/c/d/e/f) dưới đây làm đáp án của bạn cho câu hỏi này*:

a) Cắt giảm việc cung cấp thông tin sai lệch hay thông tin giả; dựa vào nguồn tin (như do chính phủ cung cấp) chính thức chi tiết, rõ ràng và minh bạch nhằm loại bỏ tin giả;
b) Ngăn chặn quyền truy cập của mọi người để xem tin tức giả mạo nơi chúng có thể xuất hiện bằng cách làm việc với các nền tảng truyền thông xã hội (như Facebook, X,…);
c) Giáo dục nhân viên đáp ứng với Nhóm A.7 Yêu cầu A.7.2 Điều A.7.2.2 Phụ lục A – ISO 27001:2013: cảnh giác với thông tin và tuân thủ chính sách ATTT của tổ chức: luôn kiểm tra tính xác thực mọi thứ xuất hiện trên màn hình máy tính (hay TV), sử dụng các trang web xác minh tính xác thực của thông tin có uy tín; xem xét kỹ lưỡng nguồn tin, sự kiện và định dạng tin;
d) Yêu cầu từng người tự hỏi xem bản thân tin vào điều này (thông tin đang lan truyền) vì sự thật phũ phàng chứng minh điều đó (“cold facts warrant it”) hay vì tôi cảm thấy dễ chịu khi tin vào điều đó?;
e) Chọn a, b, c, và d;
f) Chọn a, b và c.

14. Vào lúc 00h00 ngày 02/04/2024, hệ thống công nghệ thông tin của Tổng công ty Dầu Việt Nam (PVOil) bị tin tặc tấn công theo hình thức mã hóa dữ liệu (ransomware) khiến website, email, ứng dụng thanh toán và phát hành hóa đơn điện tử, phiếu xuất kho kiêm vận chuyển nội bộ cho khách hàng của PVOil bị ngưng hoạt động. “Ransomware” là một loại phần mềm độc hại ngăn người dùng truy cập vào thiết bị của mình và dữ liệu được lưu trữ trên thiết bị, thường bằng cách mã hóa các tệp của người dùng. Sau đó, một nhóm tội phạm sẽ yêu cầu một khoản tiền chuộc để đổi lấy việc giải mã. Không thanh toán tiền chuộc cho nhóm tội phạm này có thể dẫn đến mất dữ liệu. Những tổn thất do “ransomware” gây ra có thể rất thảm khốc. Quá trình xử lý “ransomware” thường mất nhiều tháng để phục hồi, gây ra tổn thất tài chính đáng kể và có thể đồng nghĩa với việc khôi phục dữ liệu quan trọng lại từ đầu.

Theo bạn, nhóm tội phạm “ransomware” đã khai thác yêu cầu nào trong Phụ lục A – ISO 27001:2013 theo hướng có lợi cho chúng do sự yếu kém của doanh nghiệp trong việc triển khai tuân thủ yêu cầu này - *chọn một câu trả lời (a/b/c/d) dưới đây làm đáp án của bạn cho câu hỏi này:*

a) Nhóm A.10 Yêu cầu A.10.1 Điều A.10.1.1;
b) Nhóm A.10 Yêu cầu A.10.1 Điều A.10.1.2;
c) Nhóm A.12 Yêu cầu A.12.3 Điều A.12.3.1;
d) Chọn a và c.

15. Một sự cố ATTT nghiêm trọng gây gián đoạn vận hành sàn chứng khoán đã xảy ra ở công ty chứng khoán VNX hôm 24-03-2024. Kẻ tấn công/tin tặc (“hacker”) nước ngoài đã tấn công và mã hóa hệ thống CNTT của VNX. Chủ tịch Công ty chứng khoán VNX đã xin lỗi nhà đầu tư vì sự cố gây gián đoạn, ngừng trệ giao dịch của nhà đầu tư và khách hàng của công ty dự kiến kéo dài đến ngày 01/04/2024. Bà P.M.H kể VNX đã bị bất ngờ ở những ngày đầu và phải viện đến sự hỗ trợ của các chuyên gia và công ty công nghệ hàng đầu Việt Nam, cũng như các cơ quan nhà nước. Chủ tịch Công ty chứng khoán VNX cũng nói thêm là đội ngũ VNX giỏi chuyên môn, song còn thiếu kinh nghiệm trong việc phòng bị, ngăn chặn các cuộc tấn công mạng tinh vi, ở tầm cỡ quốc tế như thế này.

Theo bạn, qua lời thú nhận trên của Bà Chủ tịch, công ty chứng khoán VNX có thể đã không đáp ứng đầy đủ được yêu cầu ATTT nào theo ISO 27001:2013 (Phụ lục A) - *chọn một câu trả lời (a/b/c/d/e/f) dưới đây làm đáp án của bạn cho câu hỏi này*:

a) Nhóm A.6 Yêu cầu A.6.1 Điều A.6.1.3 và A.6.1.4;

b) Nhóm A.12 Yêu cầu A.12.6 Điều A.12.6.1; và Nhóm A.16 Yêu cầu A.16.1 Điều A.16.1.5;

c) Nhóm A.17 Yêu cầu A.17.1 Điều A.17.1.1 và A.17.1.2;

d) Nhóm A.17 Yêu cầu A.17.2 Điều A.17.2.1;

e) Chọn a, b và d;

f) Chọn a, b, c và d.

16. Qua các trang thông tin đại chúng bạn đã nghe nói nhiều về mã độc "ransomware". Nhắc lại cho bạn nhớ: "Ransomware" là một loại phần mềm độc hại ngăn người dùng truy cập vào thiết bị của mình và dữ liệu được lưu trữ trên thiết bị, thường bằng cách mã hóa các tệp của người dùng. Sau đó, một nhóm tội phạm sẽ yêu cầu một khoản tiền chuộc để đổi lấy việc giải mã. Không thanh toán tiền chuộc cho nhóm tội phạm này có thể dẫn đến mất dữ liệu. Những tổn thất do "ransomware" gây tổn thất nhiều tỷ USD xét trên phạm vi toàn thế giới. Quá trình xử lý "ransomware" thường mất nhiều tháng để phục hồi, gây ra tổn thất tài chính đáng kể và có thể đồng nghĩa với việc khôi phục dữ liệu quan trọng lại từ đầu.

Có thể bạn cho là mình không lạ gì về mã độc hay tấn công "Ransomware". Theo bạn, mã độc nào sau đây là các dòng ("strain") hay hình thức khác nhau của "ransomware" với đặc điểm như trên - *chọn một câu trả lời (a/b/c/d/e/f) dưới đây làm đáp án của bạn cho câu hỏi này*:

a) Ryuk	b) WannaCry	c) NotPetya
d) Graboid	e) Chọn b, c và d	f) Chọn a, b và d

17. Trang báo mạng https://news.bitcoin.com/ đưa tin ngày 26/03/2024 như sau: (trích dẫn) *Telegram, một công ty cung cấp dịch vụ tin nhắn, đã bị cấm ở Tây Ban Nha sau vụ điều tra việc lưu trữ nội dung trái phép thuộc sở hữu của các công ty truyền thông ở Tây Ban Nha. Tòa án Quốc gia, một trong những tòa án cao nhất ở Tây Ban Nha, đã cho phép lệnh cấm này cho đến khi Telegram hợp tác bằng cách gửi thông tin cần thiết tới tòa án.*

Theo bạn, Telegram có thể đã không đáp ứng các yêu cầu ATTT nào trong ISO 27001:2013 (Phụ lục A) - *chọn một câu trả lời (a/b/c/d/e) dưới đây làm đáp án của bạn cho câu hỏi này*:

a) Nhóm A.15 Yêu cầu A.15.1 Điều A.15.1.2;

b) Nhóm A.18 Yêu cầu A.18.1 Điều A.18.1.2;

c) Nhóm A.18 Yêu cầu A.18.1 Điều A.18.1.3;

d) Nhóm A.18 Yêu cầu A.18.1 Điều A.18.1.4;

e) Chọn tất cả a, b, c và d.

18. Mã hóa đầu cuối ("End-to-end encryption") là một phương pháp bảo mật cho hệ thống liên lạc riêng tư trong đó chỉ những người dùng giao tiếp mới có thể tham gia. Không ai, kể cả nhà cung cấp hệ thống liên lạc, nhà cung cấp dịch vụ viễn thông, nhà cung cấp Internet hoặc tác nhân độc hại, có thể truy cập và đọc được nội dung được gửi giữa bạn và người đối thoại (hay người khác tham gia vào liên lạc). Tuy nhiên, không phải ứng dụng liên lạc nào cũng có năng lực mã hóa đầu cuối vì vậy người dùng phải tìm hiểu kỹ hoặc xin ý kiến tư vấn từ các chuyên gia bảo mật trước khi cài đặt và sử dụng một ứng dụng liên lạc riêng cho mình.

Theo bạn, xét theo khía cạnh mã hóa đầu cuối, ứng dụng liên lạc nào kém an toàn hơn trong số các ứng dụng nhắn tin sau đây và ứng dụng đó đã không đáp ứng các yêu cầu ATTT nào trong Phụ lục A – ISO 27001:2013 - *chọn một câu trả lời (a/b/c/d/e/f) dưới đây làm đáp án của bạn cho câu hỏi này*:

a) Facebook Messenger; Nhóm A.10 Yêu cầu A.10.1 Điều A.10.1.1;

b) WhatApp; Nhóm A.10 Yêu cầu A.10.1 Điều A.10.1.1;

c) Telegram; Nhóm A.10 Yêu cầu A.10.1 Điều A.10.1.1;

d) Viber; Nhóm A.10 Yêu cầu A.10.1 Điều A.10.1.1;

e) Chọn a và c;

f) Chọn b và c.

19. Single sign-on (SSO) (Đăng nhập một lần) là phương thức nhận dạng cho phép người dùng đăng nhập vào nhiều ứng dụng và trang web bằng một bộ thông tin xác thực duy nhất. SSO cho phép người dùng đăng nhập một lần và truy cập các dịch vụ / ứng dụng hay bất kỳ hệ thống phần mềm nào có liên quan nhưng độc lập mà không cần nhập lại các yếu tố xác thực. Một quản trị viên hệ thống (system admin) quản lý hàng chục hệ thống (hoặc ứng dụng hoặc dịch vụ) phải quản lý và bảo mật vài chục tài khoản đăng nhập (kèm theo mật khẩu) là thách thức cho trách nhiệm bảo mật của người này. Sử dụng SSO giúp giảm lượng thông tin xác thực bí mật mà người quản trị bắt buộc phải bảo vệ.

Theo bạn, Nhóm-Yêu cầu-Điều nào trong Phụ lục A – ISO 27001:2013 yêu cầu người dùng (Users) có trách nhiệm đảm bảo an toàn thông tin xác thực của họ và cho biết SSO có thể gây ra rủi ro tiềm ẩn gì cho hệ thống - *chọn một câu trả lời (a/b/c/d/e) dưới đây làm đáp án của bạn cho câu hỏi này*:

a) Nhóm A.9 Yêu cầu A.9.2 Điều A.9.2.4;
b) Nhóm A.9 Yêu cầu A.9.3 Điều A.9.3.1;
c) Nhóm A.9 Yêu cầu A.9.4 Điều A.9.4.2;
d) Nhóm A.9 Yêu cầu A.9.4 Điều A.9.4.3;
e) Nhóm A.18 Yêu cầu A.18.1 Điều A.18.1.3 và A.18.1.4;

Rủi ro tiềm ẩn là: ……
……

20. Trong kỳ kiểm toán ATTT tại một doanh nghiệp vào cuối năm 2021, người kiểm tra ATTT tại doanh nghiệp đã quan sát và thấy rằng bộ phận phụ trách hệ thống CNTT của doanh nghiệp đã đặt chung các thiết bị xử lý thông tin của bên thứ ba vào trong cùng một tủ Rack 42U có các máy chủ xử lý dữ liệu của doanh nghiệp. Theo giải thích của quản trị viên hệ thống ("system admin") của doanh nghiệp thì các thiết bị xử lý thông tin của bên thứ ba đặt trong tủ rack đang trong thời gian thử nghiệm tính năng trước khi doanh nghiệp sở hữu thiết bị này qua hợp đồng mua hàng. Nhân viên phụ trách hệ thống của bên thứ ba và nhân viên phụ trách hệ thống CNTT của doanh nghiệp làm việc với nhau ngay tại tủ Rack đặt tại phòng máy chủ của doanh nghiệp khi cài đặt và cấu hình thiết bị này. Theo ghi nhận của người quan sát, bên thứ ba sẽ cấp quyền truy cập vừa đủ cho doanh nghiệp để doanh nghiệp kiểm thử thiết bị trong thời gian 2 tháng.

Theo bạn, bằng việc đặt chung thiết bị xử lý thông tin của bên thứ ba (là một tổ chức bên ngoài) với thiết bị xử lý thông tin của doanh nghiệp vào cùng một tủ Rack, doanh nghiệp đã không đáp ứng yêu cầu ATTT nào trong Phụ lục A – ISO 27001:2013 - *chọn một câu trả lời (a/b/c/d) dưới đây làm đáp án của bạn cho câu hỏi này*:

a) Nhóm A.8 Yêu cầu A.8.1 Điều A.8.1.3;
b) Nhóm A.9 Yêu cầu A.9.1 Điều A.9.1.1;
c) Nhóm A.11 Yêu cầu A.11.1 Điều A.11.1.1;
d) Nhóm A.11 Yêu cầu A.11.2 Điều A.11.2.1.

21. "An Eavesdropping Attack" (một cuộc tấn công nghe lén) xảy ra khi tin tặc chặn, xóa hoặc sửa đổi dữ liệu được truyền giữa hai thiết bị. Nghe lén (hay nghe trộm), còn được gọi là đánh hơi hoặc rình mò ("sniffing or snooping"), dựa vào liên lạc mạng không bảo mật ("unsecured network communications") để truy cập dữ liệu truyền giữa các thiết bị. Nghe lén thường xảy ra khi người dùng kết nối với mạng trong đó lưu lượng truy cập không được bảo mật hoặc mã hóa và gửi dữ liệu nhạy cảm cho đồng nghiệp. Dữ liệu được truyền qua một mạng mở, tạo cơ hội cho kẻ tấn công khai thác lỗ hổng và chặn nó bằng nhiều phương pháp khác nhau. Các cuộc tấn công nghe lén thường có thể khó phát hiện. Không giống như các hình thức tấn công mạng khác, sự hiện diện của lỗi hoặc thiết bị nghe lén có thể không ảnh hưởng xấu đến hiệu suất ('performance') của thiết bị và mạng. Không có tổ chức hoặc cá nhân nào muốn nội dung trao đổi của mình với người khác bị kẻ khác nghe lén bất chấp thiệt hại lớn đến mức độ nào ở bất cứ hình thức nào.

Để phòng tránh "Eavesdropping Attack" trong môi trường làm việc tại doanh nghiệp, người kiểm tra ATTT tại doanh nghiệp quan sát và thấy rằng Trưởng Phòng ATTT của doanh nghiệp đã đề ra các biện pháp kiểm soát sau đây vào cột số (2) căn cứ theo yêu cầu ATTT theo Phụ lục A - ISO 27001:2013 – xem Bảng 1 ngay dưới đây:

Bảng 1

Stt	**Biện pháp kiểm soát**	**Nội dung trong ISO 27001:2013 có liên quan**
(1)	**(2)**	(3)

1	ENCRYPTION - Mã hóa dữ liệu truyền trên mạng	Nhóm A.13 Yêu cầu A.13.1 Điều A.13.1.3
2	SPREAD AWARENESS - Đào tạo nhận thức ATTT cho nhân viên	Nhóm A.7 Yêu cầu A.7.2 Điều A.7.2.2
3	NETWORK SEGMENTATION – Phân chia mạng	Nhóm A.10 Yêu cầu A.10.1 Điều A.10.1.1
4	AVOID SHADY LINKS – Tránh truy cập các liên kết mờ ám	Nhóm A.12 Yêu cầu A.12.2 Điều A.12.2.1; Nhóm A.12 Yêu cầu A.12.5 Điều A.12.5.1; Nhóm A.12 Yêu cầu A.12.6 Điều A.12.6.2
5	UPDATE AND PATCH SOFTWARE – Cập nhật và vá lỗi phần mềm	Nhóm A.12 Yêu cầu A.12.2 Điều A.12.2.1; Nhóm A.12 Yêu cầu A.12.5 Điều A.12.5.1; Nhóm A.12 Yêu cầu A.12.6 Điều A.12.6.1; Nhóm A.12 Yêu cầu A.12.6 Điều A.12.6.2, Nhóm A.14 Yêu cầu A.14.2 Điều A.14.2.2; Nhóm A.14 Yêu cầu A.14.2 Điều A.14.2.4;
6	PHYSICAL SECURITY – An ninh vật lý (môi trường, thiết bị…)	Nhóm A.11 Yêu cầu A.11.2 Điều A.11.2.1
7	SHIELDING TO BLOCK COMPUTER RADIATION – Tạo lớp che chắn bức xạ máy tính (ngoài ý muốn)	Nhóm A.11

Một sinh viên học ngành ATTT đã điền thông tin vào cột số (3) Bảng 1 thể hiện sự liên quan của từng Biện pháp kiểm soát ở cột số (2) với từng yêu cầu ATTT theo Phụ lục A - ISO 27001:2013.

Câu hỏi:

Với thông tin bổ sung trong cột số (3) của Bảng 1 trên, theo bạn, sinh viên trên đã sắp xếp ĐÚNG hay SAI từng biện pháp kiểm soát ở cột số (2) có liên quan với các yêu cầu ATTT trong tài liệu ISO 27001:2013 (Phụ lục A) (hoặc ISO 27002 - 2013). Nếu phát hiện ra biện pháp kiểm soát nào không có liên quan tương ứng như sắp xếp trên (hoặc liên quan SAI) thì đề nghị bạn chỉ ra cho đúng bằng cách *chọn một câu trả lời (a/b/c/d/e/f) dưới đây làm đáp án của bạn cho câu hỏi này*:

a) Liên quan SAI ở stt 1 và stt 3; hai dòng này phải hoán đổi nội dung cho nhau trong cột số (3);

b) Liên quan SAI ở stt 4 và stt 5; hai dòng này phải hoán đổi nội dung cho nhau trong cột số (3);

c) Liên quan SAI ở stt 6 và stt 7; hai dòng này phải hoán đổi nội dung cho nhau trong cột số (3);

d) Liên quan ở stt 7 bị SAI vì ISO 27001:2013 không có yêu cầu liên quan Biện pháp kiểm soát số 7;

e) Chọn a, b và d;

f) *Ghi ra chọn lựa khác của bạn:* ……..

……

22. Trước khi dịch bệnh Covid -19 bùng phát trên toàn thế giới, một quốc gia đã đầu cơ vật tư y tế bằng cách tăng cường nhập khẩu và giảm xuất khẩu vật tư y tế ra nước ngoài nhưng không một nước nào phát hiện sớm được việc đầu cơ này. Theo hãng tin AP, vào tháng 1/2020, quốc gia này đã tăng 278% số lượng khẩu trang y tế nhập khẩu, bộ quần áo phẫu thuật (tăng 72%) và găng tay phẫu thuật (tăng 32%); đồng thời nước này đã cắt giảm xuất khẩu toàn cầu đối với một loạt sản phẩm y tế như: găng tay phẫu thuật (giảm 48%), bộ quần áo phẫu thuật (giảm 71%), khẩu trang (giảm 48%), máy thở (giảm 45%), bộ dụng cụ đặt ống nội khí quản (giảm 56%), nhiệt kế (giảm 53%)…Khi dịch bệnh Covid-19 lan ra khắp thế giới thì nhiều nước lâm vào tình trạng khan hiếm hoặc không có đủ vật tư y tế và trang thiết bị y tế để phòng chống Covid-19 do đã xuất khẩu quá mức các mặt hàng này vào quốc giá đó.

Theo bạn, nếu nguồn tin trên là đúng thì điểm yếu của đa số các nước lâm vào tình trạng khan hiếm hoặc không có đủ vật tư y tế và trang thiết bị y tế để phòng chống Covid-19 là gì - *chọn một câu trả lời (a/b/c/d/e) dưới đây làm đáp án của bạn cho câu hỏi này:*

a) Quản lý dữ liệu ("Data management") vật tư y tế yếu kém: không thu thập dữ liệu, không thống kê dữ liệu, không phát hiện và tìm hiểu sự bất thường trong dữ liệu xuất nhập vật tư y tế và trang thiết bị y tế;

b) Quy định về tài sản có thiếu sót: Thông tin và dữ liệu y tế không được xem là tài sản của quốc gia dẫn đến không hoạch định hoạt động liên tục ("Business Continuity Plan") theo Nhóm A.17 Phụ lục A – ISO 27001:2013;

c) Nhận thức tình huống yếu kém: phát hiện sự tăng xuất khẩu vật tư y tế bất thường nhưng không làm gì cả;

d) Chọn a, b và c;

e) Không có điểm yếu vì dịch bệnh Covid-19 bùng phát là điều không ai có thể dự đoán trước.

23. Trong ngành hàng không có một quy tắc gọi là **"The two-person rule"**. *"This rule prevents a single individual from having unauthorized access to the cockpit. This reduces the risk of unauthorized interference or the single point of failure (SPOF). Pilots work as a team, cross-checking each other's actions and decisions. This helps prevent errors and ensures that critical tasks (such as setting altitude, speed, and navigation) are correctly executed."*. Quy tắc ("rule") này là một quy trình an toàn quan trọng trong ngành hàng không. Có hai người trong buồng lái có tác dụng bảo vệ: Có hai thành viên phi hành đoàn (thường là một phi công và một phi công phụ) đảm bảo sự an toàn do có dự phòng. Nếu một phi công mất khả năng lao động hoặc cần rời khỏi buồng lái, người còn lại có thể tiếp quản ngay lập tức. Sự dư thừa này là cần thiết để duy trì quyền kiểm soát máy bay. Trong các trường hợp khẩn cấp (chẳng hạn như có một người bị bệnh đột ngột, hỏng thiết bị hoặc sự kiện đe dọa an ninh…), việc có hai người trong buồng lái sẽ giúp đưa ra quyết định và phối hợp tốt hơn.

Bạn hãy cho biết yêu cầu và mục tiêu nào trong Phụ lục A – ISO 27001:2013 có nội dung gần gũi với quy tắc hai người "the two-person rule" - *chọn một câu trả lời (a/b/c/d/e/f) dưới đây làm đáp án của bạn cho câu hỏi này*:

a) Nhóm A.12 Yêu cầu A.12.1 Điều A.12.1.3	b) Nhóm A.12 Yêu cầu A.12.3 Điều A.12.3.1
c) Nhóm A.17 Yêu cầu A.17.2 Điều A.17.2.1	d) Nhóm A.11 Yêu cầu A.11.2 Điều A.11.2.2
e) Nhóm A.11 Yêu cầu A.11.1 Điều A.11.1.3 và A.11.1.4	f) Nhóm A.18 Yêu cầu A.18.2 Điều A.18.2.2

24. Theo yêu cầu trong Phụ lục A - ISO 27001:2013 tại Nhóm A.8 Yêu cầu A8.3 Điều A.8.3.2 thì doanh nghiệp phải thực hiện biện pháp kiểm soát (control) *"Media shall be disposed of securely when no longer required, using formal procedures."*. Bạn phụ trách hệ thống tại một công ty và công ty có nhiều ổ dĩa cứng (viết tắt là HDD – Hard Disk Drive) hư hỏng phải thanh lý bằng cách bán lại cho một số đại lý thu mua. Trước khi giao HDD cho các đại lý thu mua này, để đáp ứng yêu cầu về ATTT theo Điều A.8.3.2, bạn sẽ gì làm sau đây- *chọn một câu trả lời (a/b/c/d) dưới đây làm đáp án của bạn cho câu hỏi này*:

a) Không làm gì cả vì HDD đã bị hỏng và không ai có thể truy xuất được thông tin lưu trong HDD;

b) Nhúng HDD vào nước rồi giao cho đại lý thu mua;

c) Hỏi lại người trực tiếp sử dụng HDD để biết họ có lưu thông tin quan trọng gì không;

d) Tham khảo thủ tục loại bỏ phương tiện lưu trữ của công ty và làm theo hướng dẫn trong thủ tục.

25. Theo yêu cầu trong Phụ lục A - ISO 27001:2013 tại Nhóm A.10 Yêu cầu A.10.1 Điều A.10.1.1 và A.10.1.2 thì doanh nghiệp phải thực hiện biện pháp kiểm soát (control) để đạt mục tiêu *"To ensure proper and effective use of cryptography to protect the confidentiality, authenticity and/or integrity of information*". Để đáp ứng yêu cầu này, nhằm lưu trữ dữ liệu nhạy cảm an toàn vào phương tiện lưu trữ (HDD/CD/DVD/USB/…) và không để dữ liệu nhạy cảm của công ty bị tiết lộ ngoài ý muốn, bạn sẽ đề xuất với công ty dùng thuật toán nào sau đây để mã hóa dữ liệu - *chọn một câu trả lời (a/b/c/d/e) dưới đây làm đáp án của bạn cho câu hỏi này*:

a) MD5 (Message-Digest algorithm),

b) AES (The Advanced Encryption Standard),

c) SHA (Secure ***Hash*** Algorithm) gồm SHA-2 hoặc SHA-256,

d) DES (Data Encryption Standard),

e) Triple DES (3DES) – also known as Triple Data Encryption Algorithm (TDEA),

f) Không dùng thuật toán mã hóa dữ liệu mà bảo mật dữ liệu bằng cách khác như kiểm soát truy cập (logic và/hoặc vật lý), thuê dịch vụ lưu trữ vào đám mây của nhà cung cấp dịch vụ (ISP Cloud) v.v.

26. Theo yêu cầu trong Phụ lục A - ISO 27001:2013 tại Nhóm A.11 Yêu cầu A.11.1.6 thì doanh nghiệp phải thực hiện biện pháp kiểm soát (control)"*Access points such as delivery and loading areas and other points where unauthorized persons could enter the premises shall be controlled and, if possible, isolated from information processing facilities to avoid unauthorized access."*. Để đáp ứng yêu cầu này, khi tiếp nhận hàng hóa từ nhà cung

cấp (hay Người bán) bạn sẽ gì làm sau đây - *chọn một câu trả lời (a/b/c/d) dưới đây làm đáp án của bạn cho câu hỏi này*:

a) Cho phép Người bán giao thiết bị công nghệ thông tin (CNTT) tại phòng xử lý thông tin của bộ phận CNTT;

b) Yêu cầu Người bán giao hàng tại khu vực tiếp khách của doanh nghiệp;

c) Yêu cầu Người bán giao hàng tại khu vực đã có chỉ định của doanh nghiệp cách xa khu vực xử lý thông tin của doanh nghiệp;

d) Yêu cầu Người bán giao hàng tại nơi có ghi rõ trong Hợp đồng mua bán.

27. Theo yêu cầu trong Phụ lục A - ISO 27001:2013 tại Nhóm A.18 Yêu cầu A.18.2 Điều A.18.1.2 có yêu cầu doanh nghiệp thiết lập biện pháp kiểm soát *"Control: Appropriate procedures shall be implemented to ensure compliance with legislative, regulatory and contractual requirements related to intellectual property rights and use of proprietary soft ware products."*. Theo bạn, những hành động nào sau đây của doanh nghiệp được xem là không phù hợp với biện pháp kiểm soát trên - *chọn một câu trả lời (a/b/c/d/e/f) dưới đây làm đáp án của bạn cho câu hỏi này*:

a) Tạo ra một biểu tượng hoặc tên nhằm mục đích khiến người mua nghĩ rằng họ đang mua thương hiệu gốc;

b) Quay lại video hoặc âm nhạc mà không được phép;

c) Sao chép phần mềm, tài liệu có bản quyền (ngay cả trên máy photocopy,…) để sử dụng riêng;

d) Sử dụng từ ngữ, hình ảnh hoặc logo của người khác mà không có sự cho phép của chủ sở hữu tài sản;

e) Sao chép kiểu dáng, thương hiệu nhận dạng và giao diện người dùng của ứng dụng;

f) Chọn tất cả a, b, c, d và e.

28. Theo tin từ các trang mạng của Reuters.com, EuroNews.com, Guardian.com vào ngày 28/04/2025 (Thứ Hai), lúc 12:33 CEST (11:33 TÂY; 10:33 UTC), một vụ mất điện lớn đã xảy ra tại hai nước Bồ Đào Nha và Tây Ban Nha. Nguồn điện bị gián đoạn trong khoảng mười giờ ở hai nước này. Việc cắt điện đã gây ra những khó khăn nghiêm trọng cho viễn thông, hệ thống giao thông và các lĩnh vực thiết yếu như dịch vụ khẩn cấp. Lưu lượng truy cập Internet đã giảm mạnh 90% ở Bồ Đào Nha và 80% ở Tây Ban Nha so với mức của tuần trước. Tại Tây Ban Nha, điện đã bắt đầu trở lại xứ Basque và các khu vực Barcelona vào đầu giờ chiều cùng ngày, và một số khu vực thủ đô Madrid vào buổi tối. Khoảng 61% điện đã được phục hồi vào cuối Thứ Hai, theo nhà điều hành lưới điện quốc gia. Giới chức Tây ban nha cho biết họ đã kích hoạt các hệ thống khẩn cấp để đáp ứng nhu cầu trong thời gian mất điện và cho biết việc đưa các hệ thống trở lại bình thường sẽ mất *"vài giờ"*.

Theo bạn, căn cứ theo bản tin như trên, số giờ bị mất điện gây gián đoạn hoạt động tại hai nước được gọi là thời gian gì sau đây theo thuật ngữ của "Business Continuity Plan" - *chọn một câu trả lời (a/b/c/d) dưới đây làm đáp án của bạn cho câu hỏi này:*

a) RPO	b) RTO	c) WRT	d) MTD

29. Theo báo cáo từ Wired dựa trên phát hiện của công ty an ninh mạng Oligo được báo mạng *dantri.vn* đưa tin lại vào ngày 02/05/2025; một giao thức chia sẻ không dây AirPlay của Apple được phát hiện có lỗ hổng bảo mật nghiêm trọng. Tin tặc (kẻ tấn công) sử dụng AirPlay để phát tán phần mềm độc hại vào các thiết bị của Apple trong một số điều kiện nhất định. Nếu bị khai thác thành công, lỗ hổng này có thể cho phép kẻ tấn công thực thi các lệnh tùy ý trên thiết bị, truy cập các tệp tin nhạy cảm, hoặc thậm chí kích hoạt micro của iPhone để theo dõi người dùng. Hãng Apple đã phát hành bản vá cho lỗ hổng này thông qua các bản cập nhật phần mềm bao gồm các thiết bị chạy iOS và iPadOS 18.4; macOS 13.7.5, 14.7.5 và 15.4; cũng như visionOS 2.4.

Theo bạn, mặc dù đã có bản vá, khách hàng sử dụng thiết bị di động của Apple (như iphone, iPad,…) và thiết bị của bên thứ ba tích hợp công nghệ AirPlay vẫn có thể gặp rủi ro bị tin tặc tấn công (ứng với số RPN của rủi ro này có giá trị cao nhất) là do nguyên nhân chủ yếu nào sau đây - *chọn một câu trả lời (a/b/c/d/e/f) dưới đây làm đáp án của bạn cho câu hỏi này:*

a) Khách hàng chậm trễ cập nhật bản vá hoặc thiết bị đã ngừng nhận hỗ trợ phần mềm từ Apple;

b) Khách hàng sử dụng thiết bị của bên thứ ba tích hợp công nghệ AirPlay không được Apple kiểm soát;

c) Kẻ tấn công và thiết bị của khách hàng ở trên cùng một mạng Wi-Fi;

d) Khách hàng bật tính năng AirPlay trên thiết bị dù không sử dụng;

e) Khách hàng kết nối thiết bị với các mạng Wi-Fi công cộng;

f) *Ý kiến khác (xin ghi ra)* ……

30. Trước bối cảnh dữ liệu cá nhân (DLCN) bị lộ, lọt, mua bán tràn lan và khoảng trống pháp lý hiện tại, việc xây dựng Luật Bảo vệ DLCN được xem là vô cùng cấp thiết. Quyền riêng tư và bảo vệ thông tin nhận dạng cá nhân

sẽ được đảm bảo theo yêu cầu của luật pháp và quy định có liên quan khi Luật Bảo vệ DLCN được ban hành. Dự kiến, Luật sẽ được trình Quốc hội VN thông qua vào tháng 5/2025 và có hiệu lực từ tháng 1/2026.

Theo bạn, yêu cầu ATTT tại Điều nào trong Phụ lục A - ISO 27001:2013 và ISO 27002:2013 là cơ sở để các cá nhân và tổ chức (doanh nghiệp) mong muốn Luật DLCN được ban hành - *chọn một câu trả lời (a/b/c/d/e/f) dưới đây làm đáp án của bạn cho câu hỏi này:*

a) A.18.1.1	b) A.18.1.2	c) A.18.1.3	d) A.18.1.4	e) A.18.1.5
f) Ý kiến khác (xin ghi ra) ……..				

B. PHẦN TỰ LUẬN (10 câu)

31. Tấn công mạng ("Cyber Attack") là bất kỳ nỗ lực nào nhằm vô hiệu hóa, thao túng hoặc giành quyền truy cập trái phép vào hệ thống máy tính, mạng hoặc thiết bị. Các cuộc tấn công mạng có thể được thực hiện bởi các cá nhân, nhóm mạng hoặc thậm chí là các quốc gia và có thể nhắm mục tiêu vào các cá nhân, doanh nghiệp, chính phủ, và cơ sở hạ tầng quan trọng. Các cuộc tấn công mạng có thể dẫn đến tổn thất tài chính, vi phạm dữ liệu và thường gây thiệt hại về mặt uy tín trên quy mô lớn cho các tổ chức liên quan. Có 5 loại tấn công mạng phổ biến nhất bao gồm:

(1)Malware (Phần mềm độc hại): Phần mềm độc hại có thể được cài đặt trên máy tính mà người dùng không biết; phần mềm độc hại có thể lấy cắp dữ liệu, làm hỏng tệp hoặc làm gián đoạn hoạt động của hệ thống.

(2)Phishing (Lừa đảo): Lừa đảo trực tuyến là một loại tấn công kỹ thuật xã hội nhằm lừa người dùng tiết lộ thông tin nhạy cảm, chẳng hạn như mật khẩu hoặc số thẻ tín dụng. Các cuộc tấn công lừa đảo có thể được thực hiện thông qua email, tin nhắn văn bản hoặc thậm chí là các cuộc gọi điện thoại.

(3)Distributed Denial-of-servic (DDoS): (Tấn công từ chối dịch vụ phân tán). Tấn công DoS được thiết kế để làm tràn ngập lưu lượng truy cập vào hệ thống máy tính hoặc mạng, khiến người dùng không thể truy cập được.

(4)Man-in-the-middle (MitM) attacks (Tấn công trung gian): Tấn công MitM xảy ra khi kẻ tấn công chặn liên lạc giữa hai bên, cho phép họ nghe lén cuộc trò chuyện hoặc thậm chí sửa đổi dữ liệu được trao đổi.

(5)Zero-day attacks (Tấn công zero-day): Tấn công zero-day là các cuộc tấn công khai thác lỗ hổng trong phần mềm mà nhà cung cấp phần mềm không hề biết. Các cuộc tấn công zero-day đặc biệt nguy hiểm vì không có bản vá nào để khắc phục lỗ hổng này.

Khi được hỏi về chiến lược quản lý rủi ro ATTT đối với từng loại tấn công mạng phổ biến như trên, người kiểm tra ATTT tại doanh nghiệp nhận được kết quả như sau của doanh nghiệp – xem Bảng 1 sau đây:

Bảng 1

Loại tấn công mạng	**Chiến lược QLRR áp dụng là…**	**Chiến lược QLRR của bạn là ….**
(1)	***(2)***	***(3)***
Malware	Risk Avoidance	*(xin ghi ra ở đây)*
Phishing	Risk Transfer	*(xin ghi ra ở đây)*
DDoS	Risk Mitigation	*(xin ghi ra ở đây)*
MitM	Risk Acceptance	*(xin ghi ra ở đây)*
Zero-day	Risk Mitigation	*(xin ghi ra ở đây)*

Câu hỏi:

Bạn có hay không đồng ý với chiến lược QLRR của doanh nghiệp đề ra trong cột (2) Bảng 1 như trên.

- Nếu không đồng ý thì dựa trên 4 chiến lược QLRR có tên như trong cột số *(2)*, bạn ghi ra tên chiến lược QLRR của bạn vào cột số *(3)* trong Bảng trên.
- Nếu đồng ý với chiến lược nào ứng với loại tấn công mạng tương ứng thì bạn ghi cụm từ *"đồng ý"* vào từng dòng trong cột số *(3)* và không ghi thêm nội dung nào khác.

32. "Jamming Attacks" (tấn công gây nhiễu) là việc sử dụng sự can thiệp độc hại trên các hệ thống liên lạc không dây, bao gồm Wi-Fi, Bluetooth và mạng điện thoại di động. Hệ thống GPS cũng có thể là mục tiêu của các cuộc tấn công gây nhiễu. Mục đích của cuộc tấn công gây nhiễu là gây nhiễu mạng ("jamming a network"), ngăn chặn các thiết bị liên lạc, làm gián đoạn các dịch vụ thiết yếu hoặc thậm chí đánh sập hoàn toàn mạng trong cuộc tấn công từ chối dịch vụ (DOS). Các cuộc tấn công gây nhiễu có khả năng làm gián đoạn hoặc vô hiệu hóa hoàn toàn hoạt động liên lạc trên các mạng như Wi-Fi và Bluetooth. Điều này có thể dẫn đến mất kết nối internet và lỗi của các hệ thống dựa vào nó.

Gây nhiễu không dây là mối đe dọa nghiêm trọng đối với an ninh mạng. Để ngăn chặn các cuộc tấn công gây nhiễu không dây, Trưởng Phòng ATTT của một doanh nghiệp đã lập kế hoạch và thực hiện một số biện pháp kỹ thuật sau đây – xem cột số (2) của Bảng 1 sau đây:

Bảng 1:

Stt	**Biện pháp kỹ thuật**	**Yêu cầu ATTT liên quan**
(1)	**(2)**	(3)
1	Sử dụng các giao thức mã hóa mạnh như WPA2, WPA3 hoặc AES để bảo mật dữ liệu.	*Nhóm ..?... Yêu cầu ..?... Điều ..?...*
2	Triển khai IDS (Hệ thống phát hiện xâm nhập) có thể phát hiện tín hiệu gây nhiễu và có khả năng tự động chuyển sang các tần số và kênh thay thế.	*Nhóm ..?... Yêu cầu ..?... Điều ..?...*
3	Luôn thiết kế mạng của bạn với tính dự phòng: Sử dụng công nghệ 'Frequency Hopping' để đổi tần số hoặc truyền tín hiệu trên một băng thông rộng để tránh bị gián đoạn mạng do bị gây nhiễu.	*Nhóm ..?... Yêu cầu ..?... Điều ..?...*
4	Thường xuyên kiểm tra hệ thống, thiết bị để cập nhật chương trình và vá lỗi phần mềm.	*Nhóm ..?... Yêu cầu ..?... Điều ..?...*
5	Phân đoạn mạng: Cô lập các hệ thống quan trọng.	*Nhóm ..?... Yêu cầu ..?... Điều ..?...*
6	Bảo vệ các điểm truy cập không bị giả mạo vật lý - giữ chúng an toàn	*Nhóm ..?... Yêu cầu ..?... Điều ..?...*
7	Giáo dục/Đào tạo: Đào tạo người dùng về nhận thức về mối đe dọa	*Nhóm ..?... Yêu cầu ..?... Điều ..?...*

Yêu cầu:

Bằng hiểu biết của bạn về ISO 27001:2013, **hãy điền vào chỗ trống trong cụm từ "*Nhóm … Yêu cầu … Điều …;*" ở cột số (3) của Bảng 1** số hiệu của **ít nhất một (1)** yêu cầu ATTT nào trong Phụ lục A – ISO 27001:2013 (hoặc ISO 27002 - 2013) có biện pháp kiểm soát ("Control") liên quan đến từng biện pháp kỹ thuật mà người Trưởng Phòng ATTT của doanh nghiệp đã thực hiện.

33. Trong bối cảnh bảo mật CNTT, "Shielding" (che chắn) là từ khóa đề cập đến các kỹ thuật và biện pháp khác nhau được sử dụng để bảo vệ hệ thống thông tin và dữ liệu khỏi sự truy cập trái phép ('unauthorized access'), các cuộc tấn công và các mối đe dọa bảo mật khác. "Shielding" (che chắn) có thể bao gồm cả các biện pháp vật lý và kỹ thuật số. Bảng 1 trình bày các "Shielding" cho từng thành phần (hay đối tượng) của hệ thống thông tin như sau:

Bảng 1:

Stt	**Thành phần**	**"SHIELDING" là…**
(1)	**(2)**	(3)
1	Network (Mạng)	Tường lửa ('firewall'), hệ thống phát hiện/ngăn chặn xâm nhập ('IDS/IPS') và kiến trúc mạng an toàn ('secure network architecture') v.v.
2	Data (Dữ liệu)	Mã hóa, kiểm soát truy cập và che giấu dữ liệu ('encryption, access controls, and data masking') v.v.
3	Endpoint (Điểm cuối)	Phần mềm chống vi-rút, giải pháp phát hiện và phản hồi điểm cuối ('antivirus software, endpoint detection and response (EDR) solutions') v.v.
4	Application (Ứng dụng)	Làm xáo trộn mã, đưa ứng dụng vào danh sách trắng và sử dụng các biện pháp viết mã an toàn ('code obfuscation, application whitelisting, and the use of secure coding practices') v.v.
5	Physical (Hạ tầng vật lý như máy chủ và trung tâm dữ liệu v.v.)	Kiểm soát truy cập an toàn, giám sát và kiểm soát môi trường ('secure access controls, surveillance, and environmental controls') v.v.
6	Users (Người dùng)	Đào tạo người dùng, xác thực đa yếu tố (MFA) và các chính sách mật khẩu mạnh ('user training, multi-factor authentication (MFA), and robust password policies') v.v.

Yêu cầu:

Bằng hiểu biết của bạn về ISO 27001:2013 (hoặc ISO 27002 - 2013), hãy tự ý chọn ra 3 trong 6 thành phần nêu trên rồi GHI ra **ít nhất một (1)** yêu cầu ATTT nào trong Phụ lục A – ISO 27001:2013 có biện pháp kiểm soát

("Control") liên quan đến hoặc sử dụng "shielding" của từng thành phần trong số 3 thành phần mà bạn đã chọn theo Bảng 2 sau đây:

Stt	**Thành phần**	**"Shielding" là …**	**Yêu cầu ATTT liên quan là ….**
(1)	(2)	(3)	(4)
1	*……?……*	*(xem Bảng 1)*	*Nhóm ..?... Yêu cầu ..?... Điều ..?...*
2	*……?……*	*(xem Bảng 1)*	*Nhóm ..?... Yêu cầu ..?... Điều ..?...*
	……?……	*(xem Bảng 1)*	*Nhóm ..?... Yêu cầu ..?... Điều ..?...*

34. **MySQL** là một trong những hệ cơ sở dữ liệu (CSDL) phổ biến nhất đang được sử dụng. MySQL có hai phiên bản chính: MySQL Community Server mã nguồn mở và MySQL Enterprise Server độc quyền của Oracle. Giống như tất cả các CSDL sử dụng ngôn ngữ SQL, MySQL có một số mối đe dọa bảo mật chung với các CSDL SQL khác cũng như một số mối đe dọa riêng. Sau đây là một số mối đe dọa bảo mật phổ biến nhất đối với MySQL được liệt kê trong Bảng 1:

Bảng 1

Stt	**Các mối đe dọa cho MySQL**	**Biện pháp kiểm soát ("control") theo ISO 27001:2013 (Phụ lục A)**
(1)	**(2)**	**(3)**
1	'**Mismanagement of Account Access**': Quản lý quyền truy cập tài khoản không tốt hay chỉ định sai loại quyền truy cập tài khoản cho người dùng.	*Nhóm ..?... Yêu cầu ..?... Điều ..?...*
2	**'Weak Passwords'**: mật khẩu yếu	*Nhóm ..?... Yêu cầu ..?... Điều ..?...*
3	**'DDoS Attacks'**: tấn công DDoS Kẻ tấn công sử dụng nhiều tài khoản truy vấn giả mạo liên tiếp vào CSDL để làm chậm và cuối cùng là làm sập cơ sở dữ liệu.	*Nhóm A.9 Yêu cầu A.9.1 Điều A.9.1.1; Nhóm A.9 Yêu cầu A.9.4 Điều A.9.4.2*
4	**'SQL Injection Attacks'**: tấn công tiêm SQL Kẻ tấn công tiêm lệnh vào chuỗi truy vấn gây hư hỏng CSDL hoặc đánh cắp dữ liệu.	*Nhóm A.14 Yêu cầu A.14.2 Điều A.14.2.5, A.14.2.8*
5	**'Remote Preauth User Enumeration'**: Liệt kê người dùng xác thực trước từ xa - tấn công này được sử dụng để xác thực xem một người dùng nào đó đã có trong CSDL hay không để kẻ tấn công có thể xác định tài khoản dùng làm điểm nhập.	*Nhóm A.14 Yêu cầu A.14.2 Điều A.14.2.5, A.14.2.8*

Một nhóm sinh viên học ATTT đã tìm các Yêu cầu ATTT có biện pháp kiểm soát trong ISO 27001:2013 (Phụ lục A) (hoặc ISO 27002:2013) đáp ứng với các mối đe dọa đối với MySQL. Nhóm sinh viên này đã điền vào cột số (3) ở các hàng stt 3, 4 và 5 số hiệu của Yêu cầu ATTT đáp ứng với mối đe dọa liệt kê ở cột (2) nhưng chưa thể hoàn tất việc chỉ ra hết các Yêu cầu ATTT cho 2 mối đe dọa còn lại trong cột số (2) tại 2 hàng stt 1 và 2.

Yêu cầu:

Bằng hiểu biết của bạn về ISO 27001:2013 (hoặc ISO 27002:2013), bạn hãy:

(1) **Điền vào chỗ trống trong cụm từ "*Nhóm ? Yêu cầu ? Điều ?* " ở các hàng có stt 1 và 2 tại cột (3) - Bảng 1** số hiệu của các yêu cầu ATTT trong Phụ lục A – ISO 27001:2013 có biện pháp kiểm soát ("Control") đáp ứng với các mối đe dọa còn lại.

(*)*Yêu cầu bài làm là từng mối đe dọa trong cột (2) - Bảng 1 phải nêu ra được trong cột (3) ít nhất một yêu cầu ATTT trong ISO 27001:2013 (Phụ lục A) có biện pháp kiểm soát đáp ứng thì mới được tính điểm.*

(2) Cho ý kiến đồng ý hay không đồng ý với nội dung thông tin của Nhóm sinh viên tại các stt 3, 4 và 5:

Đồng ý: ☐	Không Đồng ý: ☐
Ý kiến khác: *(xin ghi ra)* …… …… ……	

……

35. Thống kê của công ty bảo mật Kaspersky cho thấy số vụ lây nhiễm trong các doanh nghiệp vừa và nhỏ (SMBs) trong quý I năm 2024 đã tăng 5% so với cùng kỳ năm trước; số vụ lây nhiễm phần mềm độc hại của người dùng ẩn trên thiết bị và mô phỏng phần mềm chính thống lên đến 2.402 vụ với 4.110 tệp được phân phối dưới dạng các phần mềm liên quan đến SMBs. Hình thức tấn công mạng phổ biến vẫn là Trojan. Mã độc Trojan là một công cụ phổ biến cho tội phạm mạng vì Trojan có thể lẩn trốn khỏi các công cụ an ninh mạng. Từ tháng 1 đến tháng 4 năm 2024 có tổng cộng 100.465 lượt tấn công bằng Trojan, tăng 7% so với cùng kỳ năm 2023.

Chuyên gia an ninh mạng tại Kaspersky, Ông Vasily Kolesnikov, cho biết, con người là yếu tố ảnh hưởng đến an ninh mạng của doanh nghiệp nên cần được thường xuyên nhắc nhở tuân thủ các quy tắc an ninh mạng cơ bản. Ông đề nghị doanh nghiệp các biện pháp kiểm soát sau để hạn chế các cuộc tấn công mạng – xem Bảng 1:

Bảng 1:

Stt	**Biện pháp kiểm soát**	**Yêu cầu ATTT liên quan**
(1)	**(2)**	(3)
1	Sử dụng các giải pháp bảo mật phù hợp, cung cấp khả năng bảo vệ theo thời gian thực, hiển thị mối đe dọa.	*Nhóm ..?... Yêu cầu ..?... Điều ..?...*
2	Đào tạo về an ninh mạng cho nhân viên.	*Nhóm ..?... Yêu cầu ..?... Điều ..?...*
3	Thiết lập chính sách truy cập vào tài sản của công ty, bao gồm hộp thư điện tử, thư mục dùng chung và tài liệu trực tuyến.	*Nhóm ..?... Yêu cầu ..?... Điều ..?...*
4	Cập nhật liên tục và xóa quyền truy cập khi nhân viên không còn nhu cầu sử dụng hoặc nghỉ việc.	*Nhóm ..?... Yêu cầu ..?... Điều ..?...*
5	Đảm bảo thông tin của doanh nghiệp (công ty) được an toàn trong trường hợp khẩn cấp bằng cách thường xuyên sao lưu các dữ liệu cần thiết.	*Nhóm ..?... Yêu cầu ..?... Điều ..?...*

Yêu cầu:

Bằng hiểu biết của bạn về ISO 27001:2013 (hoặc ISO 27002:2013), **hãy điền vào chỗ trống trong cụm từ *"Nhóm ? Yêu cầu ? Điều ?"* ở cột số (3) của Bảng 1** số hiệu của các yêu cầu ATTT nào trong Phụ lục A – ISO 27001:2013 có biện pháp kiểm soát ("Control") liên quan tương ứng đến từng biện pháp kiểm soát mà chuyên gia an ninh mạng của Kaspersky đã đề nghị.

(*)*Yêu cầu bài làm là từng biện pháp kiểm soát phải nêu ra được trong cột (3) ít nhất một Yêu cầu ATTT trong ISO 27001:2013 có liên quan tương ứng thì mới được tính điểm,*

36. **"Endpoint"** (Điểm cuối) là các thiết bị vật lý kết nối và trao đổi thông tin với mạng máy tính. Một số ví dụ về "endpoints" là các thiết bị di động, máy tính để bàn, máy ảo, thiết bị nhúng và máy chủ. **"Endpoint security"** (bảo mật điểm cuối) là biện pháp bảo vệ điểm cuối hoặc điểm vào của thiết bị người dùng cuối như máy tính để bàn, máy tính xách tay và thiết bị di động khỏi bị các tác nhân và chiến dịch độc hại khai thác. Hệ thống bảo mật điểm cuối bảo vệ các điểm cuối này trên mạng hoặc trên đám mây khỏi các mối đe dọa an ninh mạng. Bảo mật điểm cuối đã phát triển từ phần mềm chống vi-rút truyền thống sang cung cấp khả năng bảo vệ toàn diện khỏi phần mềm độc hại tinh vi và các mối đe dọa zero-day đang phát triển. Trang mạng https://heimdalsecurity.com/ đề nghị *"Top 10 Endpoint Security Best Practices That Help Prevent Cyberattacks"* là 10 biện pháp kiểm soát để bảo vệ "endpoints" – xem Bảng 1 sau đây:

Bảng 1:

Stt	**Biện pháp kiểm soát**	**Yêu cầu ATTT liên quan**
(1)	**(2)**	(3)
1	Keep employees security-wise	*Nhóm A.7 Yêu cầu A.7.2 Điều A.7.2.2;*
2	Apply the Principle of Least Privilege (PLP)	*Nhóm A.9 Yêu cầu A.9.2 Điều A.9.2.3;* *Nhóm A.9 Yêu cầu A.9.4 Điều A.9.4.4;*
3	Enforce USB port access policy	*Nhóm A.5 Yêu cầu A.5.1 Điều A.5.1.1;*
4	Go with the Zero Trust security model	*Nhóm A.5 Yêu cầu A.5.1 Điều A.5.1.1;*

5	Enforce a safe BYOD policy	*Nhóm A.5 Yêu cầu A.5.1 Điều A.5.1.1;*
6	Encrypt endpoints	*Nhóm ..?... Yêu cầu ..?... Điều ..?...*
7	Strengthen passwords	*Nhóm ..?... Yêu cầu ..?... Điều ..?...*
8	White/blacklisting apps	*Nhóm ..?... Yêu cầu ..?... Điều ..?...*
9	Only use VPN access for remote endpoints	*Nhóm ..?... Yêu cầu ..?... Điều ..?...*
10	Leave no door open: patch & secure all devices	*Nhóm ..?... Yêu cầu ..?... Điều ..?...*

Một nhóm sinh viên ngành ATTT đã tìm cách liên kết (hay lập mối liên quan) giữa 10 biện pháp kiểm soát của *heimdalsecurity.com* với các yêu cầu ATTT trong Phụ lục A – ISO 27001:2013. Nhóm sinh viên này đã điền vào cột số (3) ở các hàng stt 1, 2, 3, 4 và 5 nhưng chưa thể hoàn tất việc điền thông tin thể hiện sự liên kết cho 5 hàng stt còn lại là 6, 7, 8, 9 và 10.

Yêu cầu:

Bằng hiểu biết của bạn về ISO 27001:2013 (hoặc ISO 27002:2013), **hãy điền tiếp vào chỗ trống trong cụm từ "*Nhóm ? Yêu cầu ? Điều ?*" ở các hàng còn lại (stt 6, 7, 8, 9 và 10) trong cột số (3) của Bảng 1** số hiệu của các yêu cầu ATTT nào trong Phụ lục A – ISO 27001:2013 có biện pháp kiểm soát ("Control") có mối liên quan tương ứng đến từng biện pháp kiểm soát mà *heimdalsecurity.com* đề nghị.

(*) *Yêu cầu bài làm là từng biện pháp kiểm soát phải nêu ra được trong cột (3) ít nhất một yêu cầu ATTT trong ISO 27001:2013 có liên quan tương ứng thì mới được tính điểm.*

37. Mô hình Zero Trust có liên quan đến phương pháp tiếp cận "`Never trust, always verify`" (Không bao giờ tin tưởng, luôn xác minh). Theo mô hình này thì bạn không bao giờ nên tin tưởng và luôn xác minh người dùng, thiết bị, điểm cuối, mạng, ứng dụng, khối lượng công việc và luồng dữ liệu. Mô hình này đánh giá tất cả các quyền ("permissions") trước khi cấp quyền truy cập ("Access"), sau đó liên tục đánh giá lại độ tin cậy ("Trust") khi bối cảnh thay đổi. Theo trang mạng https://heimdalsecurity.com/ các đặc điểm chính của mô hình Zero Trust bao gồm việc giám sát và xác minh liên tục, nguyên tắc đặc quyền tối thiểu, phân đoạn vi mô mạng, bảo mật *'workload'*, kiểm soát việc sử dụng dữ liệu, xác thực đa yếu tố và đánh giá rủi ro – xem Bảng 1 sau đây:

Stt	**Đặc điểm của mô hình**	**Yêu cầu ATTT liên quan**
(1)	**(2)**	(3)
1	Ongoing monitoring and verification	*Nhóm ..?... Yêu cầu ..?... Điều ..?...*
2	Apply the Principle of Least Privilege (PLP)	*Nhóm ..?... Yêu cầu ..?... Điều ..?...*
3	Network micro-segmentation	*Nhóm ..?... Yêu cầu ..?... Điều ..?...*
4	Multi-factor authentication.	*Nhóm ..?... Yêu cầu ..?... Điều ..?...*
5	Workloads security (Bảo mật 'workloads') *(A workload is a computational task, process or data transaction. Workloads encompass the computing power, memory, storage and network resources required for the execution and management of applications and data. Within the cloud framework, a workload is a service, function or application that uses computing power hosted on cloud servers.)*	*Nhóm A.9 Yêu cầu A.9.4 Điều A.9.4.2;* *Nhóm A.11 Yêu cầu A.11.1 Điều A.11.1.2;* *Nhóm A.11 Yêu cầu A.11.2 Điều A.11.2.1, A.11.2.2, A.11.2.3, A.11.2.4;* *Nhóm A.10 Yêu cầu A.10.1 Điều A.10.1.1;* *Nhóm A.13 Yêu cầu A.13.1 Điều A.13.1.3*
6	Data usage controls (Kiểm soát sử dụng dữ liệu)	*Nhóm A.5 Yêu cầu A.5.1 Điều A.5.1.1;* *Nhóm A.6 Yêu cầu A.6.2 Điều A.6.2.1;* *Nhóm A.8 Yêu cầu A.8.2 Điều A.8.2.3;* *Nhóm A.8 Yêu cầu A.8.3 Điều A.8.3.1;* *Nhóm A.14 Yêu cầu A.14.3 Điều A.14.3.1;* *Nhóm A.18 Yêu cầu A.18.1 Điều A.18.1.3*
7	Threat and risk analysis (Phân tích mối đe dọa và rủi ro);	*Điều 6 khoản 6.1 điểm 6.1.1 và 6.1.2 thuộc nội dung "6 Planning" của tài liệu ISO 27001:2013;*

Một nhóm sinh viên ngành ATTT đã tìm cách liên kết (hay lập mối liên quan) giữa 6 đặc điểm của mô hình Zero Trust với các yêu cầu ATTT trong Phụ lục A – ISO 27001:2013. Nhóm sinh viên này đã điền vào cột số (3) ở các stt 5, 6 và 7 nhưng chưa thể hoàn tất việc điền thông tin thể hiện sự liên kết cho các stt còn lại là 1, 2, 3 và 4.

Yêu cầu:

Bằng hiểu biết của bạn về ISO 27001:2013 (hoặc ISO 27002:2013), **hãy điền tiếp vào chỗ trống trong cụm từ "*Nhóm ? Yêu cầu ? Điều ?*" ở các stt còn lại (stt 1, 2, 3 và 4) trong cột (3) của Bảng 1** số hiệu của các yêu cầu ATTT nào trong Phụ lục A – ISO 27001:2013 có biện pháp kiểm soát ("Control") có mối liên quan tương ứng đến từng đặc điểm của mô hình Zero Trust.

(*) *Yêu cầu là từng đặc điểm của mô hình phải nêu ra được trong cột (3) ít nhất một yêu cầu ATTT trong ISO 27001:2013 có liên quan tương ứng thì mới được tính điểm.*

38. "Coding" (tạm dịch là: *viết mã lệnh hay viết ra các lệnh*) là tạo ra một tập hợp các lệnh (hướng dẫn) để máy tính làm theo. "Coding" có nghĩa như lập trình và là một "subset of programming" và "**Secure Coding"** là viết ra các lệnh hay thảo chương sao cho an toàn. Các tiêu chuẩn của "Secure Coding" chi phối các nhà phát triển phần mềm về các thông lệ, kỹ thuật và quyết định khi "coding". "Secure Coding" nhằm mục đích đảm bảo rằng các nhà phát triển viết lệnh khi lập trình giảm thiểu lỗ hổng bảo mật trong phần mềm có thể bị khai thác bởi các mối đe dọa (như tin tặc, mã độc,…). Các tiêu chuẩn "Secure coding" khuyến khích các nhà phát triển và kỹ sư phần mềm áp dụng cách tiếp cận an toàn nhất khi lập trình phần mềm.

Hiện nay, trong số các tiêu chuẩn "Secure Coding" đang được sử dụng rộng rãi thì "OWASP Secure Coding Practices" là tiêu chuẩn được nhiều nhà phát triển phần mềm áp dụng. OWASP cung cấp danh sách kiểm tra thực hành "Secure Coding" bao gồm 14 lĩnh vực cần cân nhắc trong vòng đời phát triển phần mềm. Trong số các thực hành "Secure Coding" đó, có tám thực hành lập trình an toàn tốt nhất (*"the top eight secure programming best practices"*) để giúp lập trình viên tự bảo vệ chống lại các lỗ hổng. Tám thực hành lập trình tốt nhất được liệt kê trong Bảng 1 sau đây:

Bảng 1

Stt	**Tám (8) thực hành lập trình tốt nhất** *(the top eight secure programming best practices)* **khi thực hành "Secure Coding"**	**Yêu cầu ATTT liên quan**
(1)	**(2)**	(3)
1	Security by Design (Bảo mật theo thiết kế)	*Nhóm ..?... Yêu cầu ..?... Điều ..?...*
2	Password Management (Quản lý mật khẩu)	*Nhóm ..?... Yêu cầu ..?... Điều ..?...*
3	Access Control (Kiểm soát truy cập)	*Nhóm ..?... Yêu cầu ..?... Điều ..?...*
4	Error Handling and Logging (Xử lý lỗi và ghi nhật ký)	*Nhóm ..?... Yêu cầu ..?... Điều ..?...*
5	Cryptographic Practices (Thực hành mật mã)	*Nhóm ..?... Yêu cầu ..?... Điều ..?...*
6	Threat Modeling (Mô hình hóa mối đe dọa)	*Nhóm A.14 Yêu cầu A.14.1 Điều A.14.1.1*
7	System Configuration (Cấu hình hệ thống)	*Nhóm A.12 Yêu cầu A.12.2 Điều A.12.2.1;* *Nhóm A.12 Yêu cầu A.12.5 Điều A.12.5.1;* *Nhóm A.12 Yêu cầu A.12.6 Điều A.12.6.1;* *Nhóm A.12 Yêu cầu A.12.6 Điều A.12.6.2,* *Nhóm A.14 Yêu cầu A.14.2 Điều A.14.2.2;* *Nhóm A.14 Yêu cầu A.14.2 Điều A.14.2.4*
8	Input Validation and Output Encoding (Xác thực đầu vào và mã hóa đầu ra)	*Nhóm A.14 Yêu cầu A.14.2 Điều A.14.2.8;* *Nhóm A.14 Yêu cầu A.14.2 Điều A.14.2.9*

Một nhóm sinh viên học lập trình đã tìm cách liên kết (hay lập mối liên quan) giữa 8 "*secure programming best practices*" với các yêu cầu ATTT trong Phụ lục A – ISO 27001:2013. Nhóm sinh viên này đã điền vào cột số (3) ở các hàng stt 6, 7 và 8 nhưng chưa thể hoàn tất việc điền thông tin thể hiện sự liên kết cho 5 hàng stt còn lại là 1, 2, 3, 4 và 5. Bằng hiểu biết của bạn về ISO 27001:2013, **hãy điền vào chỗ trống trong cụm từ** *Nhóm ... Yêu cầu ....Điều....* **ở các stt 1, 2, 3, 4 và 5 tại cột (3) - Bảng 1** số hiệu của các yêu cầu ATTT trong Phụ lục A – ISO 27001:2013 có biện pháp kiểm soát ("Control") liên quan tương ứng đến từng thực hành lập trình tốt nhất.

(*)*Yêu cầu là từng thực hành lập trình tốt nhất trong cột (2)-Bảng 1 phải nêu ra được trong cột (3) ít nhất một yêu cầu ATTT trong ISO 27001:2013 (Phụ lục A) có liên quan tương ứng thì mới được tính điểm*

39. "Cloud security" (Bảo mật đám mây) là một tập hợp các biện pháp kiểm soát, chính sách và giải pháp bảo mật đám mây ("cloud security solutions") tập trung tiêu chuẩn kết hợp với nhau để bảo vệ cơ sở hạ tầng, ứng dụng và dữ liệu của bạn trên nền tảng đám mây. Theo trang https://www.esecurityplanet.com, mặc dù đã có giải pháp bảo mật đám mây nhưng vẫn có một số thách thức và rủi ro mà các tổ chức phải đối mặt khi bảo vệ dữ liệu của họ trên đám mây như trong Bảng 1 sau đây:

Bảng 1

Stt	**Năm thách thức và rủi ro hàng đầu trong bảo mật đám mây** *(5 Top Challenges & Risks of Cloud Security)*	**Biện pháp kiểm soát ("control") theo ISO 27001:2013 (Phụ lục A)**
(1)	**(2)**	(3)
1	Misconfiguration (Cấu hình sai)	*Nhóm ..?... Yêu cầu ..?... Điều ..?...*
2	Unauthorized Access (Truy cập trái phép)	*Nhóm ..?... Yêu cầu ..?... Điều ..?...*
3	Hijacking of Accounts (Chiếm đoạt tài khoản)	*Nhóm ..?... Yêu cầu ..?... Điều ..?...*
4	External Sharing of Data (Chia sẻ dữ liệu bên ngoài)	*Nhóm ..?... Yêu cầu ..?... Điều ..?...*
5	Unsecured Third-Party Resources (Tài nguyên của bên thứ ba không an toàn)	*Nhóm ..?... Yêu cầu ..?... Điều ..?...*

Một nhóm sinh viên học ATTT đã tìm các biện pháp kiểm soát trong Phụ lục A – ISO 27001:2013 để đối phó với 5 thách thức nêu trên. Nhóm sinh viên này đã điền vào cột số (3) ở hàng stt 5 nhưng chưa thể hoàn tất việc điền thông tin thể hiện các biện pháp kiểm soát cho 4 thách thức còn lại tại 4 hàng stt 1, 2, 3 và 4. Bằng hiểu biết của bạn về ISO 27001:2013, **hãy điền vào chỗ trống trong cụm từ** *Nhóm ... Yêu cầu ....Điều....* **ở các stt 1, 2, 3 và 4 tại cột (3) - Bảng 1** số hiệu của các yêu cầu ATTT trong Phụ lục A – ISO 27001:2013 có biện pháp kiểm soát ("Control") đối phó với các thách thức tương ứng.
(*)*Yêu cầu là từng thách thức trong cột (2) - Bảng 1 phải nêu ra được trong cột (3) ít nhất một yêu cầu ATTT trong ISO 27001:2013 (Phụ lục A) có biện pháp kiểm soát đối phó phù hợp thì mới được tính điểm.*

40. Được thúc đẩy bởi quảng cáo về tính hiệu quả, khả năng mở rộng và tốc độ đổi mới được tăng cường, điện toán đám mây đã trở nên quá lớn đến nỗi 95% khối lượng công việc mới vào năm 2025 được dự đoán sẽ được triển khai trên đám mây. Tuy nhiên, theo trang https://hadrian.io/blog/, quá trình triển khai này cũng gây ra những rủi ro bảo mật mới phải được doanh nghiệp quản lý cẩn thận để bảo vệ dữ liệu nhạy cảm và duy trì tính toàn vẹn của hoạt động như trong Bảng 1 sau đây:

Bảng 1

Stt	**Năm rủi ro tiềm ẩn hàng đầu trong bảo mật đám mây** *(Top 5 Hidden Cloud Risks)*	**Biện pháp kiểm soát ("control") theo ISO 27001:2013 (Phụ lục A)**
(1)	**(2)**	(3)
1	Lack of visibility (Thiếu khả năng hiển thị)	*Nhóm ... Yêu cầu ....Điều....*
2	Misconfiguration (Cấu hình sai),	*Nhóm ... Yêu cầu ....Điều....*
3	Lack of encryption (Thiếu mã hóa)	*Nhóm ... Yêu cầu ....Điều....*
4	Zero-day vulnerabilities (Lỗ hổng zero-day)	*Nhóm ... Yêu cầu ....Điều....*
5	Unsecured APIs (API không an toàn)	*Nhóm ... Yêu cầu ....Điều....*

Một nhóm sinh viên học ATTT đã tìm các biện pháp kiểm soát trong Phụ lục A – ISO 27001:2013 để tránh hoặc giảm nhẹ rủi ro nêu trên. Nhóm sinh viên này đã điền vào cột số (3) ở hàng stt 5 số hiệu của Yêu cầu ATTT đối phó với rủi ro "Unsecured APIs" nhưng chưa thể hoàn tất việc điền thông tin thể hiện các biện pháp kiểm soát cho 4 rủi ro tiềm ẩn còn lại tại 4 hàng stt 1, 2, 3 và 4. Bằng hiểu biết của bạn về ISO 27001:2013, **hãy điền vào chỗ trống trong cụm từ** *Nhóm ... Yêu cầu ....Điều....* **ở các stt 1, 2, 3 và 4 tại cột (3) - Bảng 1** số hiệu của các yêu cầu ATTT trong Phụ lục A – ISO 27001:2013 có biện pháp kiểm soát ("Control") đối phó với các rủi ro còn lại.
(*)*Yêu cầu là từng rủi ro tiềm ẩn trong cột (2) - Bảng 1 phải nêu ra được trong cột (3) ít nhất một yêu cầu ATTT trong ISO 27001:2013 (Phụ lục A) có biện pháp kiểm soát đối phó phù hợp thì mới được tính điểm.*

---------- Hết ----------