HỌC VIỆN KTQS
KHOA CÔNG NGHỆ THÔNG TIN

Bài 4.
Quản lý rủi ro

Học phần: BẢO ĐẢM VÀ AN TOÀN THÔNG TIN

NỘI DUNG

1. Giới thiệu
2. Xác định rủi ro
3. Đánh giá rủi ro
4. Chiến lược kiểm soát rủi ro
5. Thảo luận, bài tập

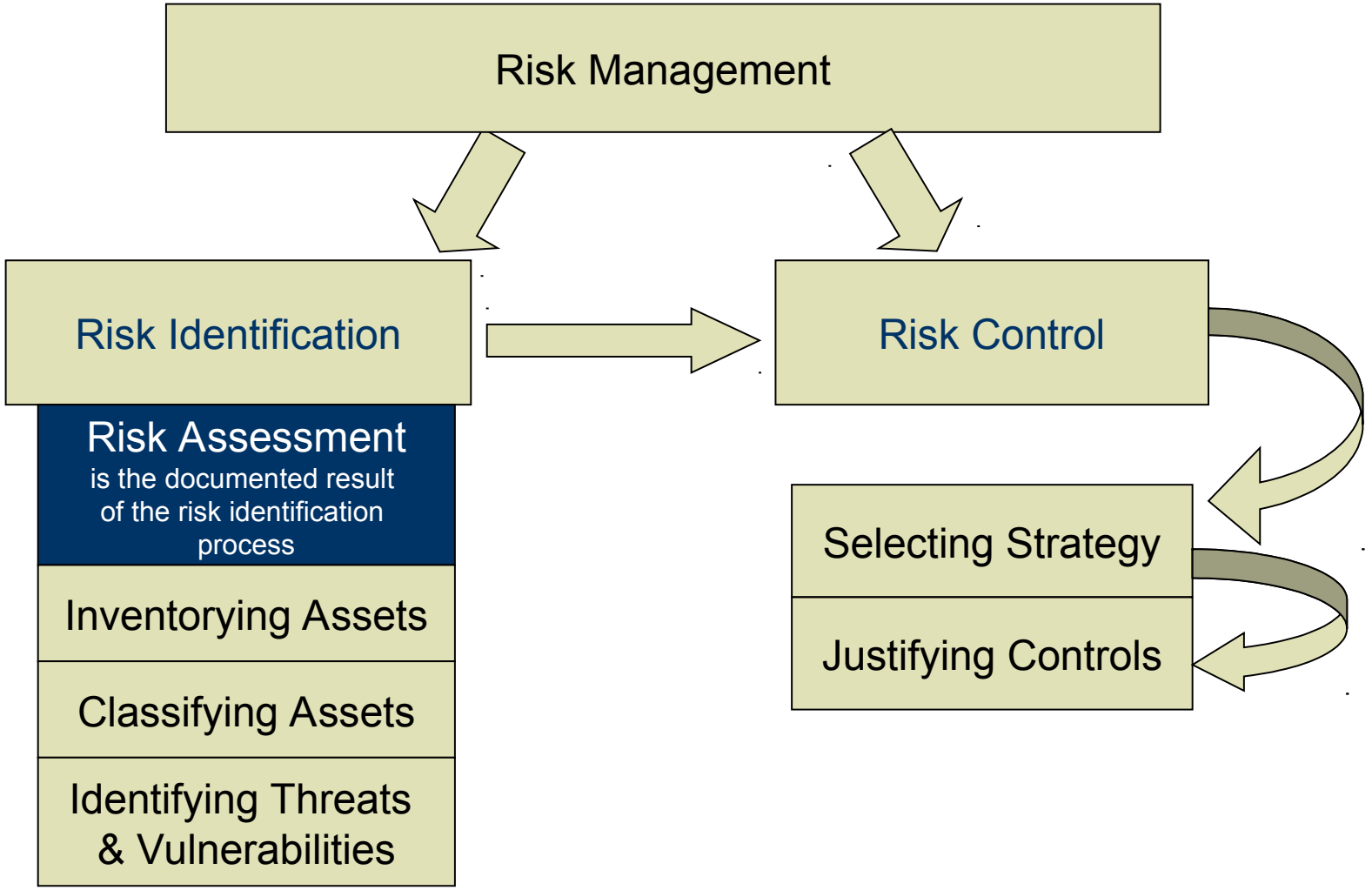
1. Giới thiệu

Quản lý rủi ro: là quy trình xác định và kiểm soát rủi ro mà một tổ chức có thể đối mặt

Xác định rủi ro: là quy trình kiểm tra tình hình an ninh của hệ thông tin hiện tại của tổ chức

Kiểm soát rủi ro: là quy trình áp dụng các biện pháp kiểm soát để giảm rủi ro cho một hệ thống thông tin và dữ liệu của tổ chức

Các thành phần trong quản lý rủi ro



Tổng quan về quản lý rủi ro

Hiểu bản thân: nắm bắt được công nghệ và hệ thống thông tin trong tổ chức

Hiểu được đối thủ: xác định, kiểm tra, và hiểu được các mối đe dọa

Vai trò của cộng đồng:

- bảo mật thông tin
- quản lý và người dùng
- công nghệ thông tin

2. Xác định rủi ro

- Tài sản là mục tiêu của nhiều mối đe dọa
- Quản lý rủi ro liên quan tới việc xác định tài sản của hệ thống và xác định các mối đe dọa và điểm yếu của các tài sản đó
- Xác định rủi ro bắt đầu bằng việc xác định các tài sản của hệ thống và đánh giá giá trị của chúng

Xác định rủi ro

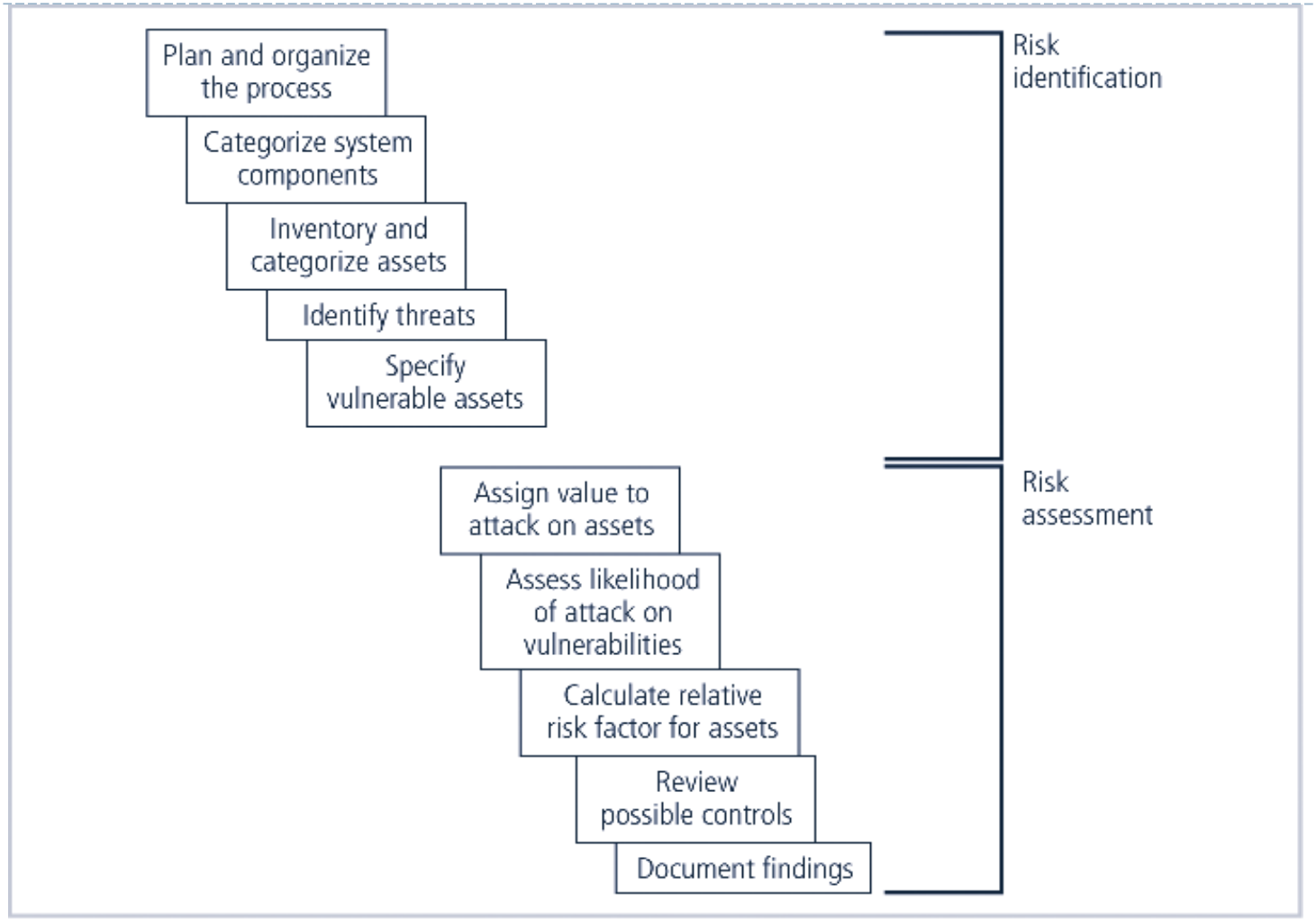


FIGURE 4-2 Components of Risk Identification

Xác định tài sản và định giá

- Xác đinh tài sản là một quá trình lặp lại, trong đó việc xác định tài sản bao gồm các yếu tố con người, thủ tục, dữ liệu và thông tin, phần mềm, phần cứng, mạng..
- Tài sản sau khi được xác định sẽ được phân loại

Xác định tài sản và định giá

Traditional System Components	SecSDLC and risk management system components	
People	Employee	Trusted employees Other staff
	Non-employees	People at trusted organizations / Strangers
Procedures	Procedures	IT & business standards procedures IT & business standards procedures
Data	Information	Transmission, Processing, Storage
Software	Software	Applications, Operating systems, Security components
Hardware	System devices and peripherals	Systems and peripherals Security devices
	Networking components	Intranet components Internet or DMZ components

Con người, thủ tục, tài sản dữ liệu

- Nguồn tài nguyên con người, tài liệu, tài sản dữ liệu là các tài sản khó xác định
- Xác định thuộc tính cho con người bao gồm: tên, ID, vị trí trong hệ thống, người giám sát, mức độ bảo mật mà người đó đảm nhiệm, các kỹ năng đặt biệt của người đó.
- Xác định thuộc tính cho thủ tục: xác định mục đích; mối quan hệ với phần mềm, phần cứng, các phần tử mạng trong hệ thống; Khu vực lưu trữ
- Xác định thuộc tính cho dữ liệu hệ thống: phân loại dữ liệu dựa trên người sở hữu, người tạo, người quản lý; cấu trúc kích thước của dữ liệu, cấu trúc được sử dụng như on-offline, thủ tục sao lưu được sử dụng

Tài sản phần cứng, phần mềm, mạng

- Số serial
- Tên, bộ phần, mô hình của nhà sản xuất
- Phiên bản phần mềm, phiên bản update
- Vị trí vật lý, logic trong hệ thống
- Thực thể kiểm soát nó: đơn vị mà nó trực thuộc

Phân lớp tài sản

- Phân lớp tài sản theo các lược đồ (tính bảo mật, dữ liệu trong hay ngoài hệ thống, dữ liệu đó có được công bố hay bảo mật)
- Phân lớp phải đủ đặc biệt để xác định được độ ưu tiên
- Tính toàn diện: tất cả các thông tin phải phù hợp với dánh sách nó được đưa vào
- Tính loại trừ lẫn nhau: thông tin chỉ phù hợp với 1 vị trí mà nó được đưa vào

Phân lớp tài sản

- Lược đồ GP (Georgia-Pacific Corporation)
+ Bảo mật, nhạy cảm hoặc độc quyền
+ Nhân viên nội bộ, G-P, nhà thầu được ủy quyền

Bên ngoài, công khai

- Lược đồ (US military)
+ Dữ liệu chưa được phân loại
+ Độ nhạy cảm của dữ liệu chưa được phân loại
+ Dữ liệu bảo mật
+ Dữ liệu bí mật hàng đầu

Phân lớp tài sản

Các tổ chức có thể cần phải phân loại dữ liệu theo các tiêu chí sau:

- Mức độ Công bố
- Chỉ dùng cho nhân viên
- Mức độ nhạy cảm
- Dữ liệu đã được phân loại

Phân lớp tài sản

- Phân lớp tài sản cho tất cả dữ liệu hệ thống
- Cấp quyền truy cập dựa trên việc phân lớp và sự cần thiết của người dùng
- Đưa ra một số phương pháp quản lý liên quan tới việc phân lớp

Quản lý tài sản

- Xem xét các vấn đề về lữu trữ, phân phối, tiêu hủy tài sản nếu cần
- Thông tin không được phân loại, hoặc được công khai, phải được đánh dấu rõ ràng
- Các thông tin được lưu trữ trong vị trí lưu trữ hàng ngày, các thông tin không cần thiết cần được xóa bỏ

Định giá tài sản

Xây dựng các tiêu chí thông qua các câu hỏi:

- Tài sản đó có quan trọng đối với sự thành công của tổ chức không?
- Tài sản đó tạo ra doanh thu như thế nào?
- Tài sản đó có lợi nhuận như thế nào?
- Tài sản đó khi thay thế có đắt không?
- Tài sản đó khi cần bảo vệ có chi phí lớn không?
- Khi nó bị tiết lộ thì ảnh hưởng như thế nào?

Định giá tài sản

System Name: SLS E-Commerce
Date Evaluated: February 2003
Evaluated By: D. Jones

Information assets	Data classification	Impact to profitability
Information Transmitted:		
EDI Document Set 1 —Logistics BOL to outsourcer (outbound)	Confidential	High
EDI Document Set 2—Supplier orders (Outbound)	Confidential	High
EDI Document Set 2—Supplier fulfillment advice (inbound)	Confidential	Medium
Customer order via SSL (inbound)	Confidential	Critical
Customer service Request via e-mail (inbound)	Private	Medium
DMZ Assets:		
Edge Router	Public	Critical
Web server #1—home page and core site	Public	Critical
Web server #2—Application server	Private	Critical

Notes: BOL: Bill of Lading:
DMZ: Demilitarized Zone
EDI: Electronic Data Interchange
SSL: Secure Sockets Layer

Example Worksheet for the Asset Identification of Information Systems

Sắp xếp tài sản theo mức độ quan trọng

- Phân tích trọng số
- Gán điểm cho các yếu tố ảnh hưởng theo từng tiêu chí, giá trị trong đoạn [0-1] :
- Các tiêu chí: ảnh hưởng tới doanh thu, lợi nhuận, và hình ảnh công bố
- Mỗi tiêu chí được gán điểm [1-100]
- Trọng số của các yếu tố ảnh hưởng là tổng điểm theo các tiêu chí

Sắp xếp tài sản theo mức độ quan trọng

TABLE 4-2 Example of a Weighted Factor Analysis Worksheet

Information asset	Criteria 1: impact to revenue	Criteria 2: impact to profitability	Criteria 3: public image impact	Weighted score
Criterion Weight (1-100) Must total 100	30	40	30	
EDI Document Set 1—Logistics BOL to outsourcer (outbound)	0.8	0.9	0.5	75
EDI Document Set 2—Supplier orders (outbound)	0.8	0.9	0.6	78
EDI Document Set 2—Supplier fulfillment advice (inbound)	0.4	0.5	0.3	41
Customer order via SSL (inbound)	1.0	1.0	1.0	100
Customer service request via e-mail (inbound)	0.4	0.4	0.9	55

Notes: EDI: Electronic Data Interchange
SSL: Secure Sockets Layer

Các mối đe dọa

Type of Attack or Misuse	2009	2008	2007	2006	2005	2004	2003	2002	2001	2000
Theft of or unauthorized access to IP due to mobile device theft or loss	6%	4% (new in 2008)								
Theft of or unauthorized access to PII or PHI due to mobile device theft or loss	6%	8% (new in 2008)								
Extortion or blackmail associated with threat of attack or release of stolen data	3% (new in 2009)									
These categories were replaced or dropped in subsequent years										
Unauthorized access to information		29%	25%	32%	32%	37%	45%	38%	49%	71%
Theft or loss of customer or employee data		17%	17% (new in 2007)							
System penetration		13%	13%	15%	14%	17%	36%	40%	40%	25%
Misuse of public Web applications		11%	9%	6%	5%	10% (new in 2004)				
Theft or loss of proprietary information		9%	8%	9%	9%	10%	21%	20%	26%	20%
Telecommunications fraud		5%	5%	8%	10%	10%	10%	9%	10%	11%
Sabotage		2%	4%	3%	2%	5%	21%	8%	18%	17%
Telecomm eavesdropping							6%	6%	10%	7%
Active wiretap							1%	1%	2%	1%

Table 4-5 CSI Survey Results for Types of Attack or Misuse (2000–2009) (continued)

Các mối đe dọa

Ranking of Top Threats Based on Money and Effort Spent to Defend Against or React to the Threat	2009 Ranking	2003 Ranking
Espionage or trespass	1	6
Software attacks	2	1
Missing, inadequate, or incomplete controls	3	—
Theft	4	7
Quality of service deviations by service providers	5	5
Forces of nature	6	10
Sabotage or vandalism	7	8
Technological obsolescence	8	9
Technical software failures or errors	9	3
Technical hardware failures or errors	10	4
Compromises to intellectual property	11	11
Human error or failure	12	2
Missing, inadequate, or incomplete organizational policy or planning	13	—
Information extortion	14	12

Table 4-6 Weighted Ranking of Top Threat-Driven Expenditures

Đánh giá các mối đe dọa

- Mối đe dọa thực tế cần điều tra; các mối đe dọa không quan trọng sẽ được xem xét sau

+ Mỗi xử lý phải kiểm tra đánh giá tiềm năng thiệt hại

+ Chi phí để phục hồi hệ thống nếu đe dọa xảy ra

+ Chi phí để ngăn trặn các đe dọa đó

Xác định các điểm yếu (lỗ hổng)

- Xác định đối với mỗi tài sản, thì phải đối mặt với các đe dọa nào
- Tạo danh sách các điểm yếu
- Kiểm tra xem các đe dọa đó sẽ xảy ra như thế nào

3. Đánh giá rủi ro

- Đánh giá rủi ro là việc đánh giá từng điểm yếu mà có thể dẫn tới rủi ro đó
- Gán điểm rủi ro cho từng tài sản theo công thức:

Rủi ro = khả năng xảy ra rủi ro * giá trị tài sản - phần trăm của các giảm thiểu rủi ro bởi các kiểm soát hiện tại + Sự không hiểu biết chắc chắn về các lỗ hổng hiện tại

Khả năng rủi ro

- Là xác suất của một lỗ hổng cụ thể bị đối phương khai thác hoặc tấn công thành công
- Khả năng sẽ nhận giá trị trong đoạn [0.1, 1]
- Ví dụ: dữ liệu luôn luôn đối mặt với các yếu tố như:
    + Khả năng hỏa hoạn
    + Khả năng nhận các thư điện tử chứa mã độc
    + Các cuộc tấn công mạng

Định giá trị cho các tài sản thông tin

- Sử dụng các thông tin từ tài sản để đánh trọng số giá trị cho tài sản
- Giá trị trong khoảng [1, 100]
- 100 có nghĩa là hệ thống ngừng hoạt động

Xác định khả năng kiểm soát các lỗ hổng

- Với mỗi mối đe dọa đưa ra danh sách các ý tưởng có thể kiểm soát được
- Ước lượng rủi ro còn lại sau khi đã thực hiện các kiểm soát

Bài toán

- Bài toán 1: Tài sản A có điểm giá trị là 50, có 1 lỗ hổng. Lỗ hổng 1 có khả năng xảy ra là 1.0 và hiện tại chưa có kiểm soát nào cho lỗ hổng này, Bạn ước tính giả định với độ chính xác là 90%

- Bài toán 2: Tài sản B có điểm giá trị là 50, có 2 lỗ hổng. Lỗ hổng 2 có khả năng là 0.5 với ước lượng kiểm soát hiện tại là 50%. Lỗ hổng 3 có khả năng là 0.1 và chưa có kiểm soát hiện tại nào. Bạn ước lượng giả định rủi ro với độ chính xác 80%

Lời giải

Rủi ro = khả năng xảy ra rủi ro * giá trị tài sản - phần trăm của các giảm thiểu rủi ro bởi các kiểm soát hiện tại + Sự không hiểu biết chắc chắn về các lỗ hổng hiện tại

Rủi ro của A= (50 X 1.0)–(50 X 1.0) X0% + (50 X 1.0) X10%

= (50 X 1.0)– ((50 X 1.0)X0) +((50 X 1.0)+.1)

= 50 – 0 + 5 = 55

Rủi ro của B (V2)= (100 X .5)– (100 X .5) X50% + (100 X .5) X20%

= 50- 25 + 10 = 35

Rủi ro của B (V3)= (100 X .1)– 0% + (100 X .1) X20%

= 10 – 0 + 2 = 12

Tài liệu hóa kết quả đánh giá rủi ro

Tài liệu hóa theo bảng biểu về các loại tài sản, mức độ ảnh hưởng của tài sản, các lỗ hổng, khả năng xảy ra của các lỗ hổng, và sự ảnh hưởng của rủi ro đó

Tài liệu hóa kết quả đánh giá rủi ro

Asset	Asset Impact or Relative Value	Vulnerability	Vulnerability Likelihood	Risk-Rating Factor
Customer service request via e-mail (inbound)	55	E-mail disruption due to hardware failure	0.2	11
Customer order via SSL (inbound)	100	Lost orders due to Web server hardware failure	0.1	10
Customer order via SSL (inbound)	100	Lost orders due to Web server or ISP service failure	0.1	10
Customer service request via e-mail (inbound)	55	E-mail disruption due to SMTP mail relay attack	0.1	5.5
Customer service request via e-mail (inbound)	55	E-mail disruption due to ISP service failure	0.1	5.5
Customer order via SSL (inbound)	100	Lost orders due to Web server denial-of-service attack	0.025	2.5
Customer order via SSL (inbound)	100	Lost orders due to Web server software failure	0.01	1

Table 4-9 Ranked Vulnerability Risk Worksheet

4. Chiến lược kiểm soát rủi ro

Khi sắp xếp xong các rủi ro theo mức độ quan trong, chúng ta phải chọn một trong 4 chiến lược sau để kiểm soát:

1. Tránh rủi ro bằng cách xóa bỏ, hoặc giảm các rủi ro. Ví dụ: chặn email ngoài Internet
2. Chuyển rủi ro ra khỏi hệ thống, hoặc bên thứ 3: Ví dụ mua bảo hiểm
3. Giảm ảnh hưởng của các rủi ro
4. Chấp nhận rủi ro (Hiểu rủi ro nhưng vẫn chấp nhận)

Tránh rủi ro

- Ngăn ngừa việc thực thi các lỗ hổng
- Kiểm soát các mối đe dọa, loại bỏ các tài sản có chứa lỗ hổng, giới hạn truy cập, thêm các biện pháp bảo vệ bằng bộ phận bảo vệ
- 3 phương pháp:
    + Áp dụng các chính sách
    + Đào tạo và giáo dục
    + Áp dụng các công nghệ bảo mật mới

Chuyển đổi rủi ro

Bằng cách chuyển các rủi ro cho một bên khác :
- Xem xét lại cách dịch vụ được cung cấp
- Sửa đổi các mô hình triển khai
- Gia công phần mềm
- Mua bảo hiểm
- Thực hiện hợp đồng dịch vụ

Giảm thiểu rủi ro

Giảm rủi ro là giảm ảnh hưởng của các lỗ hổng thông qua các kế hoạch và chuyển bị:

- Kế hoạch phản hồi lại các biến cố
- Kế hoạch phục hồi thảm họa
- Kế hoạch công việc liên tục

Chấp nhận rủi ro

- Không làm gì cả, chập nhận khi rủi ro đến:
- Tình huống xảy ra khi việc đánh đổi chi phí cho việc áp dụng các biện pháp kiểm soát rủi ro cao hơn chính tài sản của hệ thống khi thay thế mới

Lựa chọn chiến lược kiểm soát rủi ro

- Lựa chọn các mối đe dọa, và giá trị tài sản đóng vai trò quyết định trong lựa chọn chiến lược:
+ Khi có 1 lỗ hổng, thực hành các kiểm soát để giảm thiểu khả năng của lỗ hổng đó
+Khi một lỗ hổng có thể được khai thác - áp dụng bảo vệ lớp, thiết kế kiến trúc và điều khiển quản trị
+ Khi chi phí của kẻ tấn công ít hơn lợi nhuận tiềm năng - hãy áp dụng biện pháp bảo vệ để tăng chi phí cho kẻ tấn công
+ Khi mất tiềm năng là đáng kể - thiết kế lại kiến trúc mới, điều khiển mới

Vòng đời kiểm soát rủi ro

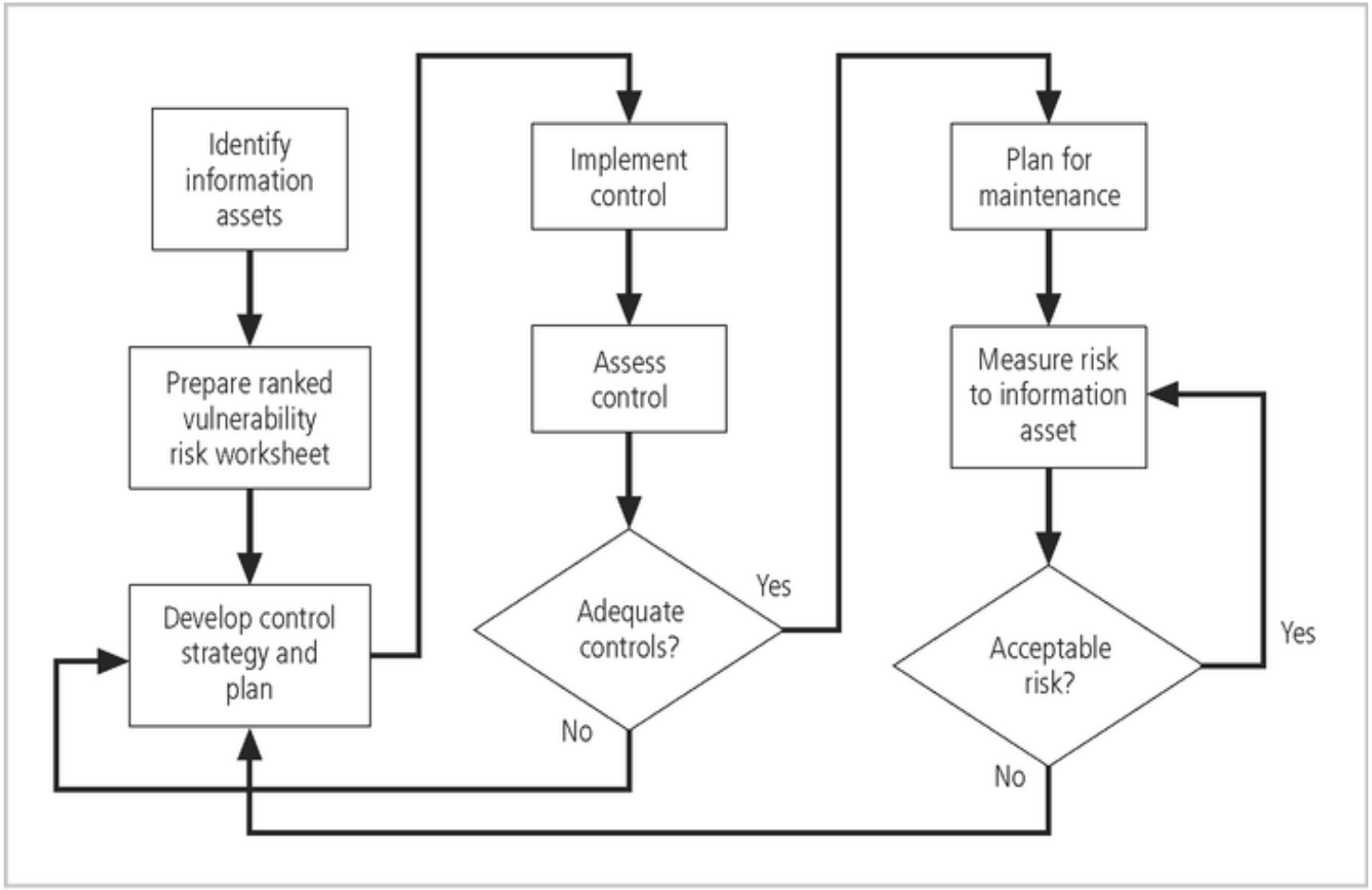


FIGURE 5-3 Risk Control Cycle[8]

Danh mục kiểm soát

- Chức năng điều khiển: ngăn ngừa & xác định
- Lớp kiến trúc: Chính sách tổ chức, mạng bên ngoài, mạng nội bộ, thiết bị mạng, hệ thống
- Lớp chiến lược: Tránh, giảm thiểu hoặc chuyển đổi
- Nguyên tắc bảo mật thông tin: Được phân loại theo các đặc điểm: Bảo mật, tính toàn vẹn, tính khả dụng, xác thực, ủy quyền, trách nhiệm, riêng tư

Danh mục kiểm soát

- Chức năng điều khiển: ngăn ngừa & xác định
- Lớp kiến trúc: Chính sách tổ chức, mạng bên ngoài, mạng nội bộ, thiết bị mạng, hệ thống
- Lớp chiến lược: Tránh, giảm thiểu hoặc chuyển đổi
- Nguyên tắc bảo mật thông tin: Được phân loại theo các đặc điểm: Bảo mật, tính toàn vẹn, tính khả dụng, xác thực, ủy quyền, trách nhiệm, riêng tư

Phân tích lợi ích chi phí(CBA)

- Đánh giá giá trị của tài sản
- Giá trị mất mát nếu tài sản bị thỏa hiệp
- Công thức tính kỳ vọng mất mát đơn:

  SLE = asset value * exposure factor

  Exposure factor = % loss from exploitation
- Kỳ vọng mất mát hàng năm:

  ALE = SLE * ARO (Tỉ lệ hằng năm xảy ra)
- Hạng mục ảnh hưởng tới chi phí điều khiển:
  - Chi phí phát triển hoặc mua lại
  - Chi phí thực hiện
  - Chi phí dịch vụ
  - Chi phí bảo trì

Công thức tính lợi ích chi phí (CBA)

- CBA xác định có hay không kiểm soát thay thế đang được đánh giá là giá trị phát sinh để kiểm soát lỗ hổng

Công thức:

CBA = ALE (prior) – ALE (post) – ACS

- ALE (trước) là kỳ vọng mất mát hàng năm của rủi ro trước khi thực hiện kiểm soát
- ALE (sau) được ước tính ALE dựa trên sự kiểm soát được đặt ra trong một khoảng thời gian
- ACS là chi phí bảo vệ hàng năm
- CBA >0: nên áp dụng chính sách, ngược lại thì không áp dụng chính sách đó.

5. Bài tập

Bài 1: Công ty X có doanh thu 1.200.000USD. Tính ARO và ALE đối với từng đe dọa.

Threat Category	Cost per Incident (SLE)	Frequency of Occurrence
Programmer mistakes	$5,000	1 per week
Loss of intellectual property	$75,000	1 per year
Software piracy	$500	1 per week
Theft of information (hacker)	$2,500	1 per quarter
Theft of information (employee)	$5,000	1 per six months
Web defacement	$500	1 per month
Theft of equipment	$5,000	1 per year
Viruses, worms, Trojan horses	$1,500	1 per week
Denial-of-service attacks	$2,500	1 per quarter
Earthquake	$250,000	1 per 20 years
Flood	$250,000	1 per 10 years
Fire	$500,000	1 per 10 years

5. Bài tập

Bài 2: Công ty X sau khi áp dụng các biện pháp kiểm soát an ninh trong 1 năm.Sử dụng bảng dưới đây tính giá trị post-ARO and post-ALE sau khi công ty áp dụng các kiểm soát, tính lợi ích chi phí và khuyến X nên thực hiện chính sách kiểm soát đối với đe dọa nào.

Threat Category	Cost per Incident	Frequency of Occurrence	Cost of Control	Type of Control
Programmer mistakes	$5,000	1 per month	$20,000	Training
Loss of intellectual property	$75,000	1 per 2 years	$15,000	Firewall/IDS
Software piracy	$500	1 per month	$30,000	Firewall/IDS
Theft of information (hacker)	$2,500	1 per 6 months	$15,000	Firewall/IDS
Theft of information (employee)	$5,000	1 per year	$15,000	Physical security
Web defacement	$500	1 per quarter	$10,000	Firewall
Theft of equipment	$5,000	1 per 2 years	$15,000	Physical security
Viruses, worms, Trojan horses	$1,500	1 per month	$15,000	Antivirus
Denial-of-service attacks	$2,500	1 per 6 months	$10,000	Firewall
Earthquake	$250,000	1 per 20 years	$5,000	Insurance/backups
Flood	$50,000	1 per 10 years	$10,000	Insurance/backups
Fire	$100,000	1 per 10 years	$10,000	Insurance/backups

HỎI VÀ ĐÁP