# QUẢN LÝ AN TOÀN THÔNG TIN

Giảng viên: Nguyễn Ngọc Điệp

Bộ môn ATTT – Khoa CNTT1

## Top-paying certifications:

1. **Google Certified Professional Data Engineer** — $171,749
2. **Google Certified Professional Cloud Architect** — $169,029
3. **AWS Certified Solutions Architect - Associate** — $159,033
4. **CRISC - Certified in Risk and Information Systems Control** — $151,995
5. **CISSP - Certified Information Systems Security Professional** — $151,853
6. **CISM – Certified Information Security Manager** — $149,246
7. **PMP® - Project Management Professional** — $148,906
8. **NCP-MCI - Nutanix Certified Professional - Multicloud Infrastructure** — $142,810
9. **CISA - Certified Information Systems Auditor** — $134,460
10. **VCP-DVC - VMware Certified Professional - Data Center Virtualization 2020** — $132,947
11. **MCSE: Windows Server** — $125,980
12. **Microsoft Certified: Azure Administrator Associate** — $121,420
13. **CCNP Enterprise - Cisco Certified Network Professional - Enterprise** — $118,911
14. **CCA-V - Citrix Certified Associate - Virtualization** — $115,308
15. **CompTIA Security+** — $110,974

https://www.globalknowledge.com/us-en/resources/resource-library/articles/top-paying-certifications/#gref

# Nghề nghiệp trong lĩnh vực bảo mật thông tin

Hầu hết các nghiên cứu / báo cáo đều chỉ ra sự thiếu hụt các chuyên gia bảo mật trong vòng 5 năm tới.

Báo cáo của tờ New York Times, năm 2021 cần:

- 3,5 triệu công việc An ninh mạng toàn cầu

# 10 Popular Cybersecurity Certifications [2021 Updated]

| Certification | LinkedIn | Indeed | Simply Hired | Total |
|---|---|---|---|---|
| CISSP | 48,711 | 13,499 | 9,333 | 71,543 |
| CISA | 12,466 | 6,138 | 3,859 | 22,463 |
| CISM | 8,860 | 4,064 | 2,806 | 15,730 |
| Security+ | 5,371 | 3,583 | 2,698 | 11,652 |
| CEH | 5,894 | 2,401 | 1,697 | 9,992 |
| GSEC | 3,633 | 2,515 | 1,897 | 8,045 |
| SSCP | 3,682 | 2,442 | 1,859 | 7,983 |
| CASP | 2,918 | 2,052 | 1,500 | 6,470 |
| GCIH | 2,872 | 1,902 | 1,279 | 6,053 |
| OSCP | 2,798 | 1,948 | 949 | 5,695 |

*Number of US job search results for each certification when searched on June 10, 2021*

**Certified Information Systems Security Professional (CISSP)**
for experienced security professionals in roles like:
•Chief information security officer - $170,793
•Security administrator - $85,742
•IT security engineer - $100,605
•Senior security consultant - $111,250
•Information assurance analyst - $82,070

**CISSP**

- Certified Information Systems Security Professional
- Highly advanced and most sought-after cyber security credential for experienced professionals
- Create and formulate IT security policies, standards, and procedures

https://www.coursera.org/articles/popular-cybersecurity-certifications

# Certified Information Systems Security Professional


**The Certification That Inspires Utmost Confidence**

5 năm kinh nghiệm trong lĩnh vực bảo mật thông tin
Có 250 câu hỏi trắc nghiệm
Thời lượng kiểm tra: sáu giờ

# 10 Popular Cybersecurity Certifications [2021 Updated]

| Certification | LinkedIn | Indeed | Simply Hired | Total |
|---|---|---|---|---|
| CISSP | 48,711 | 13,499 | 9,333 | 71,543 |
| CISA | 12,466 | 6,138 | 3,859 | 22,463 |
| CISM | 8,860 | 4,064 | 2,806 | 15,730 |
| Security+ | 5,371 | 3,583 | 2,698 | 11,652 |
| CEH | 5,894 | 2,401 | 1,697 | 9,992 |
| GSEC | 3,633 | 2,515 | 1,897 | 8,045 |
| SSCP | 3,682 | 2,442 | 1,859 | 7,983 |
| CASP | 2,918 | 2,052 | 1,500 | 6,470 |
| GCIH | 2,872 | 1,902 | 1,279 | 6,053 |
| OSCP | 2,798 | 1,948 | 949 | 5,695 |

*Number of US job search results for each certification when searched on June 10, 2021*

**Certified Information Systems Auditor (CISA)**
designed for mid-level IT professionals looking to advance into jobs like:
•IT audit manager - $122,254
•Cybersecurity auditor - $69,083
•Information security analyst - $99,372
•IT security engineer - $93,526
•IT project manager - $102,743
•Compliance program manager - $92,829

https://www.coursera.org/articles/popular-cybersecurity-certifications

# 10 Popular Cybersecurity Certifications [2021 Updated]

| Certification | LinkedIn | Indeed | Simply Hired | Total |
|---|---|---|---|---|
| CISSP | 48,711 | 13,499 | 9,333 | 71,543 |
| CISA | 12,466 | 6,138 | 3,859 | 22,463 |
| CISM | 8,860 | 4,064 | 2,806 | 15,730 |
| Security+ | 5,371 | 3,583 | 2,698 | 11,652 |
| CEH | 5,894 | 2,401 | 1,697 | 9,992 |
| GSEC | 3,633 | 2,515 | 1,897 | 8,045 |
| SSCP | 3,682 | 2,442 | 1,859 | 7,983 |
| CASP | 2,918 | 2,052 | 1,500 | 6,470 |
| GCIH | 2,872 | 1,902 | 1,279 | 6,053 |
| OSCP | 2,798 | 1,948 | 949 | 5,695 |

*Number of US job search results for each certification when searched on June 10, 2021*

**Certified Information Security Manager (CISM)**
pivot from the technical to the managerial side of cybersecurity.
•IT manager - $108,353
•Information systems security officer - $96,568
•Information risk consultant - $92,624
•Director of information security - $173,387
•Data governance manager - $119,816

**CISM program**
•information security strategy development
•selecting and appropriate risk governance frameworks
•choosing the right organizational structure and roles establish incident management process

https://www.coursera.org/articles/popular-cybersecurity-certifications

# 10 Popular Cybersecurity Certifications [2021 Updated]

| Certification | LinkedIn | Indeed | Simply Hired | Total |
|---|---|---|---|---|
| CISSP | 48,711 | 13,499 | 9,333 | 71,543 |
| CISA | 12,466 | 6,138 | 3,859 | 22,463 |
| CISM | 8,860 | 4,064 | 2,806 | 15,730 |
| Security+ | 5,371 | 3,583 | 2,698 | 11,652 |
| CEH | 5,894 | 2,401 | 1,697 | 9,992 |
| GSEC | 3,633 | 2,515 | 1,897 | 8,045 |
| SSCP | 3,682 | 2,442 | 1,859 | 7,983 |
| CASP | 2,918 | 2,052 | 1,500 | 6,470 |
| GCIH | 2,872 | 1,902 | 1,279 | 6,053 |
| OSCP | 2,798 | 1,948 | 949 | 5,695 |

*Number of US job search results for each certification when searched on June 10, 2021*

**Certified Ethical Hacker (CEH)**
•Penetration tester - $104,116
•Cyber incident analyst - $86,454
•Threat intelligence analyst - $90,269
•Cloud security architect - $158,536
•Cybersecurity engineer - $100,636

**CEH**

- Certified Ethical Hacker
- Learn to hack networks and systems ethically
- Perform penetration testing to find and fix vulnerabilities in networks and systems

**ECSA**

- EC-Council Certified Security Analyst
- Next level cert after CEH
- Conduct analysis and perform intensive assessments on networks and systems

https://www.coursera.org/articles/popular-cybersecurity-certifications

# CompTIA Security +

Chứng nhận nghề ban đầu

Yêu cầu 2 năm kinh nghiệm làm việc trong lĩnh vực An toàn mạng

Người có chứng chỉ có chuyên môn trong các lĩnh vực kiến thức như

- Mật mã học
- Quản lý danh tính
- Hệ thống An toàn
- Nhận dạng và giảm thiểu rủi ro bảo mật
- Kiểm soát truy cập mạng

# Nội dung môn học Quản lý ATTT

Cung cấp các kiến thức căn bản và giới thiệu các vấn đề thực tiễn trong việc xây dựng và quản lý các giải pháp đảm bảo an toàn thông tin nhằm đáp ứng yêu cầu an toàn của cơ quan/tổ chức. Cụ thể:

- Các tiêu chuẩn an toàn phổ biến
- Quy định pháp luật về an toàn thông tin trong nước và quốc tế
- Phương pháp xác định và đánh giá rủi ro nhằm giảm thiểu tác động của các lỗ hổng an toàn thông tin
- Nguyên tắc và biện pháp giúp cho việc vận hành hệ thống đảm bảo an toàn, duy trì việc hoạt động liên tục và cách ứng phó khi có sự cố an toàn thông tin.

# Nội dung

**Chương 1: Tổng quan về quản lý an toàn thông tin**

1.1 Giới thiệu về quản lý an toàn thông tin
1.2 Chính sách và luật pháp an toàn thông tin
1.3 Các nguyên tắc trong quản lý an toàn thông tin
1.4 Phân loại thông tin và hệ thống thông tin
1.5 Các biện pháp quản lý ATTT
1.6 Tổ chức quản lý ATTT

# Nội dung

**Chương 2: Hệ thống pháp luật ATTT của Việt Nam và các nước**

2.1 Các yêu cầu về pháp luật, chính sách

2.2 Các luật về ATTT của Việt Nam

2.3 Hệ thống pháp luật ATTT của các nước

2.3.1 Luật pháp ATTT của Mỹ

2.3.2 Luật pháp ATTT của Châu Âu

2.3.3 Luật pháp ATTT của các nước trong khu vực

# Nội dung

**Chương 3: Hệ thống tiêu chuẩn ATTT**

3.1 Hệ thống tiêu chuẩn ATTT trên thế giới

3.1.1 Hệ thống tiêu chuẩn ISO/IEC

3.1.2 Hệ thống tiêu chuẩn NIST

3.2 Hệ thống tiêu chuẩn ATTT của Việt Nam

# Nội dung

**Chương 4: Hệ thống quản lý ATTT**

4.1 Bộ khung quản lý ATTT

4.2 Quản lý rủi ro

4.3 Nhận dạng, phân tích và đánh giá rủi ro

4.4 Các chiến lược kiểm soát rủi ro

4.5 Các thực tế về kiểm soát rủi ro

# Nội dung

**Chương 5: Quản lý vận hành khai thác an toàn**

5.1 Nguyên tắc quản lý vận hành an toàn

5.2 Quản lý cấu hình

5.3 Kiểm soát thiết bị, dữ liệu

5.4 Trách nhiệm trong quản lý vận hành, khai thác

# Nội dung

**Chương 6: Duy trì hoạt động và khắc phục sự cố**

6.1 Nguyên tắc duy trì hoạt động và khắc phục sự cố

6.2 Xây dựng kế hoạch duy trì hoạt động

6.3 Chiến lược khôi phục sự cố

6.4 Kiểm thử và cập nhật kế hoạch

# Tài liệu tham khảo


Michael E. Whitman and Herbert J. Mattord, *Management of Information Security*, Course Technology, Cengage Learning, 2010.

Michael E. Whitman, Herbert J. Mattord, *Roadmap to Information Security: For IT and Infosec Managers*, Delmar Publishers Inc., 2011.

Sari Greene, *Security Policies and Procedures Principles and Practices*, Prentice Hall, 2005.

Michael E. Whitman, Herbert J. Mattord, *Principles of information security, 4th edition*, Course Technology, Cengage Learning, 2012.

# ĐÁNH GIÁ MÔN HỌC

- Các điểm thành phần:
  - Chuyên cần: 10%
  - Kiểm tra: 10%
  - Bài tập+Tiểu luận: 20%
  - Thi cuối kỳ: 60%

# Trao đổi về lớp học

Nội quy
Lớp trưởng
Facebook group
Online classroom

# Đề cương khóa học - Các chủ đề được cập nhật

- Lập kế hoạch cho Bảo mật và Dự phòng
- Chính sách an toàn thông tin
- Phát triển chương trình đảm bảo an toàn
- Mô hình quản lý an toàn
- Quản lý rủi ro
  - Phát hiện
  - Đánh giá
  - Kiểm soát

# Đề cương khóa học - Các chủ đề được đề cập

- Cơ chế bảo vệ
- Nhân sự và An toàn
- Luật và Đạo đức
- Bảo mật và Đám mây

# Chủ đề hiện tại / Tự nghiên cứu về Quản lý ATTT

- Mục đích là tự tìm hiểu 1 vấn đề trong quản lý an toàn thông tin trong số các vấn đề của môn học.

- Làm slide và báo cáo .

# Chủ đề hiện tại / Dự đoán về mối đe dọa

- Mục đích chính là đưa ra các chủ đề hiện tại đang xảy ra trong thế giới an toàn thông tin.

- Chọn 1 dự đoán mối đe dọa cho năm 2021 để nghiên cứu và trình bày trong một trong các buổi học.

# Thực hành / Trình bày demo

Chuẩn bị bài thuyết trình (5-7 phút) và trình diễn trực tiếp hoặc bài tập thực hành trong phòng thực hành (20-25 phút) về công nghệ liên quan đến bảo mật.

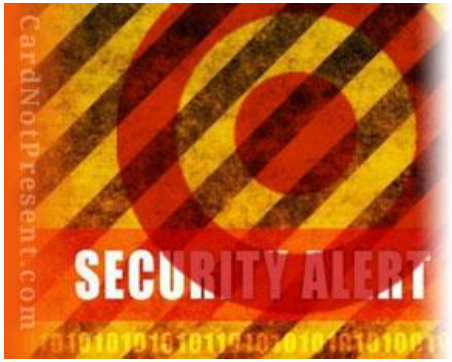
Bao gồm:

- Báo cáo
- Thuyết trình trên lớp
- Demo

# Quản lý an toàn thông tin

Bạn có thể có tất cả các cơ chế bảo vệ mà vẫn gặp sự cố bảo mật:

# Quản lý an toàn thông tin




http://www.twincities.com/business/ci_24887125/target-breach-liilities-an-inside-job-data-security

http://www.computerweekly.com/news/2240212475/Target-to-invest-5m-in-cyber-security-awareness

http://uckyne.com/2014/12/30/new-research-sony-hack/

http://www.techrepublic.com/article/why-the-sony-hack-shouldnt-lead-to-the-end-of-user-centric-it/



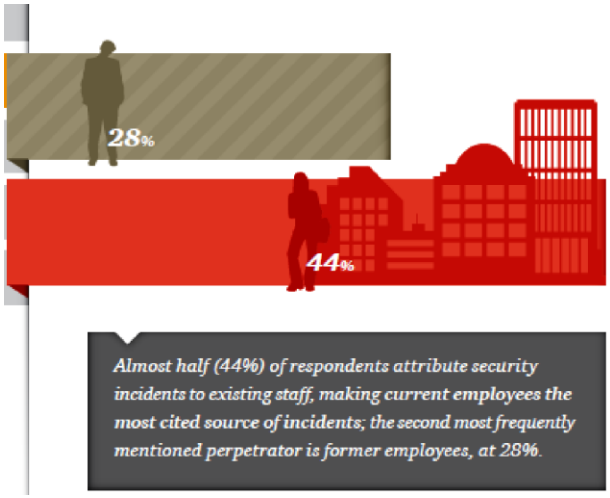
http://www.businessweek.com/articles/2014-11-06/home-depot-hackers-got-in-via-a-vendor-took-53-million-e-mails-too

# Công nghệ là không đủ… ..
(Theo: PWC Global State of Information Security 2015)

Ngay cả những giải pháp công nghệ tốt nhất cũng đang được nghiên cứu liên tục để vượt qua.

Các quy trình quản trị và hoạt động thiết yếu:

- Quy trình ứng phó quản lý sự cố
- Phân loại giá trị kinh doanh của dữ liệu
- Đánh giá rủi ro trên hệ thống nội bộ
- Kiểm tra bảo mật
- Quản trị, rủi ro và tuân thủ



# Quản lý An toàn Thông tin
(Từ: PWC Global State of Information Security 2014)

## *The fundamental safeguards you'll need for an effective security program.*

Effective security requires implementation of numerous technical, policy, and people safeguards. Based on a regression analysis of survey responses and PwC's experience in global security practices, the following are ten key strategies.

| Essential safeguards for effective security | |
|---|---|
| 1 | A written security policy |
| 2 | Back-up and recovery/business continuity plans |
| 3 | Minimum collection and retention of personal information, with physical access restrictions to records containing personal data |
| 4 | Strong technology safeguards for prevention, detection, and encryption |
| 5 | Accurate inventory of where personal data of employees and customers is collected, transmitted, and stored, including third parties that handle that data |
| 6 | Internal and external risk assessments of privacy, security, confidentiality, and integrity of electronic and paper records |
| 7 | Ongoing monitoring of the data-privacy program |
| 8 | Personnel background checks |
| 9 | An employee security awareness training program |
| 10 | Require employees and third parties to comply with privacy policies |

September 2013

# Quản lý an toàn thông tin

Mục tiêu của khóa học này là lùi lại một bước và kiểm tra cách thức hoạt động của ATTT nói chung trong tổ chức.

**Thử thách:**

Mọi thứ không thể được phân loại là đúng hay sai

Những gì hiệu quả cho một công ty này có thể thất bại ở một công ty khác

# Các hình thức bảo mật thông tin ban đầu

Earlier versions of the German code machine Enigma were first broken by the Poles in the 1930s. The British and Americans managed to break later, more complex versions during World War II. The increasingly complex versions of the Enigma, especially the submarine or *Unterseeboot* version of the Enigma, caused considerable anguish to Allied forces before finally being cracked. The information gained from decrypted transmissions was used to anticipate the actions of German armed forces. "Some ask why, if we were reading the Enigma, we did not win the war earlier. One might ask, instead, when, if ever, we would have won the war if we hadn't read it."[1]

Hình 1-1: Máy Enigma

# Những năm 1990

Mạng máy tính trở nên phổ biến hơn; vì vậy cũng cần phải kết nối các mạng

Internet trở thành biểu hiện đầu tiên của một mạng lưới toàn cầu

Trong những lần triển khai Internet ban đầu, ATTT được coi là mức độ ưu tiên thấp

# 2000 đến nay

Internet đưa hàng triệu mạng máy tính vào giao tiếp với nhau — nhiều mạng trong số đó không được bảo mật

Khả năng bảo mật dữ liệu của máy tính bị ảnh hưởng bởi tính bảo mật của mọi máy tính mà nó được kết nối

Mối đe dọa ngày càng tăng của các cuộc tấn công mạng đã làm tăng nhu cầu cải thiện mức độ an ninh

# Giới thiệu

Khái niệm bảo mật máy tính đã trở thành đồng nghĩa với khái niệm an toàn thông tin

**An toàn thông tin không còn là trách nhiệm duy nhất của một nhóm người rời rạc trong công ty**

# Người ra quyết định về an toàn thông tin

**1) Người quản lý an toàn thông tin và các chuyên gia**

(Cộng đồng InfoSec)

**2) Người quản lý công nghệ thông tin và các chuyên gia**

(Cộng đồng Công nghệ Thông tin)

**3) Người quản lý kinh doanh phi kỹ thuật và các chuyên gia**

(Cộng đồng Doanh nghiệp Tổng hợp)

# ATTT là gì?

- Bạn định nghĩa ATTT như thế nào?

- Các lĩnh vực ATTT chuyên biệt
  - Vật lý
  - Hoạt động
  - Thông tin liên lạc
  - Mạng

**Mỗi lĩnh vực này đều đóng góp vào chương trình an toàn thông tin nói chung**

# An toàn thông tin là gì?

## Làm thế nào để chúng ta đạt được An toàn Thông tin?

- Chính sách
- Công nghệ
- Các chương trình đào tạo và nâng cao nhận thức

**Vai trò của an toàn thông tin là bảo vệ tài sản thông tin của tổ chức**

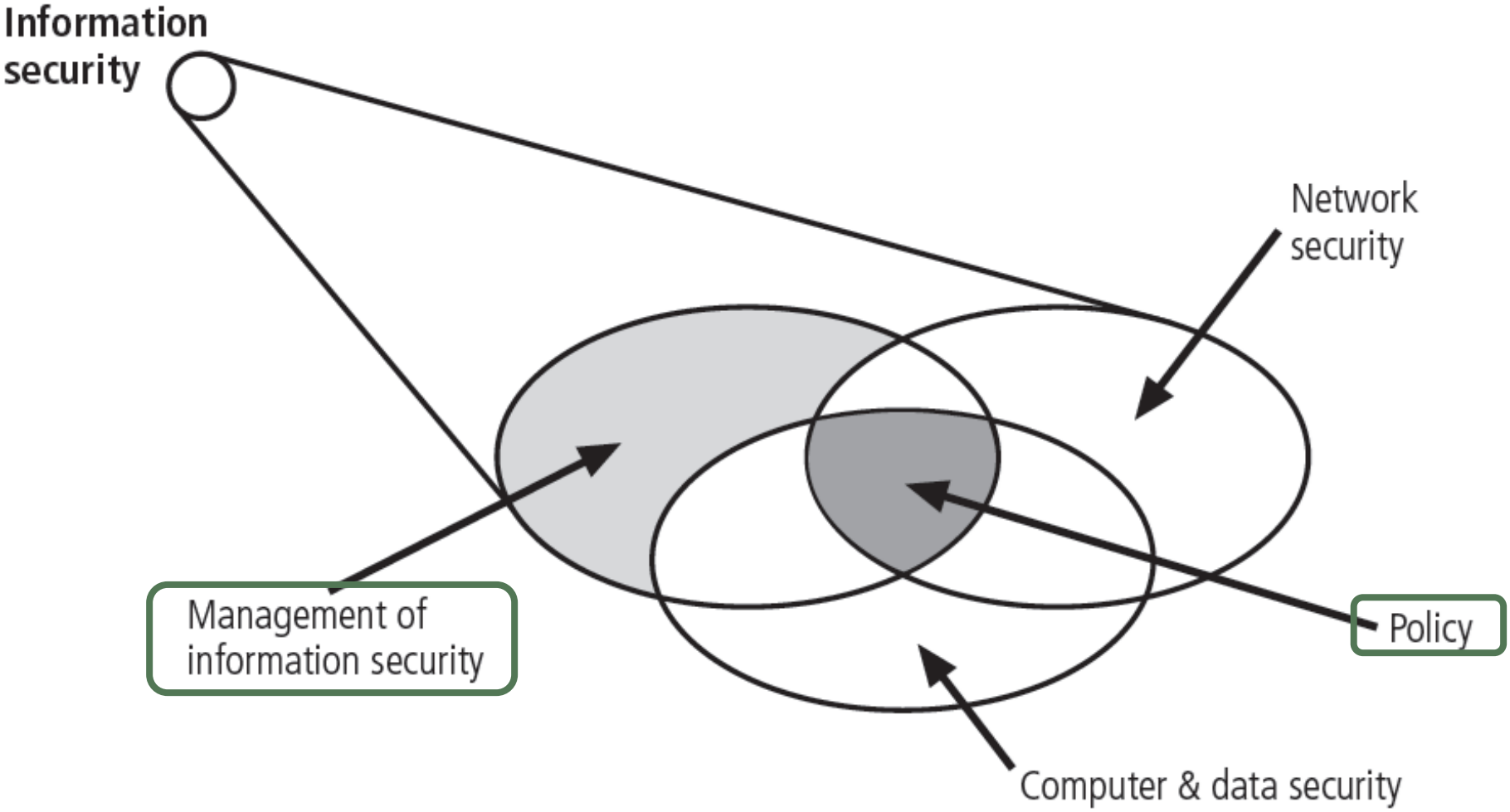
# Các thành phần của hệ thống thông tin

Hệ thống thông tin (IS) là toàn bộ tập hợp các thành phần cần thiết để sử dụng thông tin như một nguồn lực trong tổ chức

- Phần mềm
- Phần cứng
- Dữ liệu
- Con người
- Thủ tục
- Mạng

# Các khái niệm chính về an toàn thông tin

- Truy cập
- Tài sản
- Tấn công
- Kiểm soát, Bảo vệ hoặc Biện pháp đối phó
- Khai thác
- Phơi bày
- Mất mát
- Hồ sơ bảo vệ
- Rủi ro
- Chủ thể và đối tượng
- Nguy cơ
- Tác nhân đe dọa
- Lỗ hổng




http://www.cnss.gov/policies.html

# Mô hình an toàn CNSS (tiếp theo)

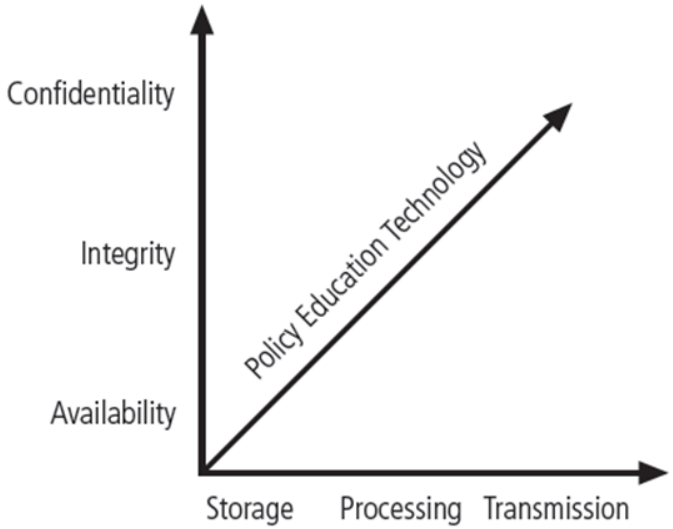
- Tam giác C.I.A.
  - Tính bí mật, tính toàn vẹn và tính sẵn sàng/khả dụng
  - Đã mở rộng thành danh sách toàn diện hơn về các đặc điểm quan trọng của thông tin

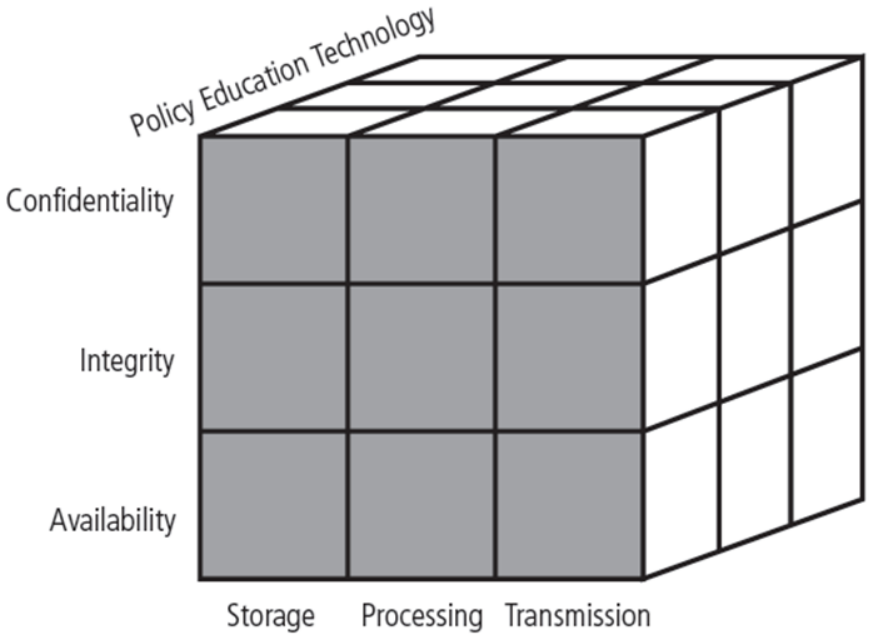
- Mô hình an toàn NSTISSI (CNSS)
  - Cung cấp quan điểm chi tiết hơn về an toàn
  - Bao gồm ba khía cạnh của an toàn thông tin
  - Mục đích chính: xác định các lỗ hổng trong phạm vi bao phủ của một chương trình an toàn thông tin

# Mô hình an toàn CNSS (tiếp theo)

- Mô hình an toàn NSTISSC (tiếp theo)

Phải giải quyết tất cả 27 ô khi thiết kế / xem xét một chương trình




**Mục đích chính: xác định các lỗ hổng trong chương trình an toàn thông tin**

# Cách đo giá trị của thông tin - Tam giác CIA

Giá trị của thông tin đến từ những đặc điểm mà nó sở hữu


**Đã mở rộng, bao gồm**

**Identification**
**Authentication**
**Authorization**
**Privacy**
**Accountability**

# Tính bí mật

Đặc điểm của thông tin theo đó chỉ những người có đủ đặc quyền mới có thể truy cập vào một số thông tin nhất định

**Các biện pháp được sử dụng để bảo vệ bí mật:**

- Phân loại thông tin
- Lưu trữ tài liệu an toàn
- Áp dụng các chính sách bảo mật chung
- Giáo dục người quản lý thông tin và người dùng cuối

# Tính toàn vẹn

Chất lượng hoặc trạng thái là toàn bộ, hoàn chỉnh và không bị gián đoạn

**Các mối đe dọa đối với tính toàn vẹn của thông tin:**

- Bị hỏng
- Tổn hại
- Sự phá hủy
- Sự gián đoạn khác của trạng thái xác thực của nó

# Tính sẵn sàng/khả dụng

Đặc tính của thông tin cho phép người dùng truy cập thông tin ở định dạng được yêu cầu, không bị can thiệp hoặc cản trở

Tính sẵn sàng không có nghĩa là thông tin có thể truy cập được đối với bất kỳ người dùng nào (Hàm ý tính sẵn sàng đối với người dùng được ủy quyền)

# Nhận dạng và xác thực

**Nhận dạng**

- Một hệ thống thông tin có tính năng nhận dạng khi nó có thể nhận ra người dùng cá nhân
- Nhận dạng và xác thực là điều cần thiết để thiết lập cấp độ truy cập hoặc ủy quyền mà một cá nhân được cấp

**Xác thực**

- Xảy ra khi kiểm soát chứng minh rằng người dùng sở hữu danh tính mà họ tuyên bố

# Ủy quyền

Đảm bảo rằng người dùng đã được bên có thẩm quyền thích hợp cho phép cụ thể và rõ ràng để truy cập, cập nhật hoặc xóa nội dung của tài sản thông tin

**Ủy quyền xảy ra sau khi xác thực**

# Sự riêng tư

- Thông tin do một tổ chức thu thập, sử dụng và lưu trữ chỉ được sử dụng cho các mục đích đã nêu với chủ sở hữu dữ liệu tại thời điểm nó được thu thập

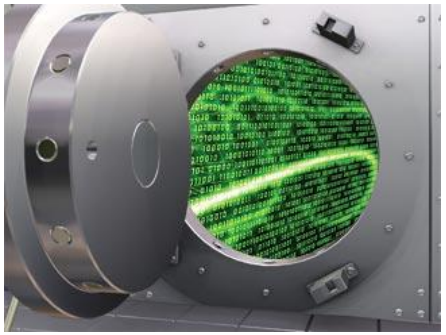
- Quyền riêng tư khi được xem xét là một đặc tính của thông tin không có nghĩa là tự do quan sát
  - Có nghĩa là thông tin sẽ chỉ được sử dụng theo những cách mà người cung cấp thông tin đó biết

# Trách nhiệm giải trình

Tồn tại khi một biện pháp kiểm soát cung cấp đảm bảo rằng mọi hoạt động được thực hiện có thể được quy cho một người được chỉ định hoặc tiến trình tự động

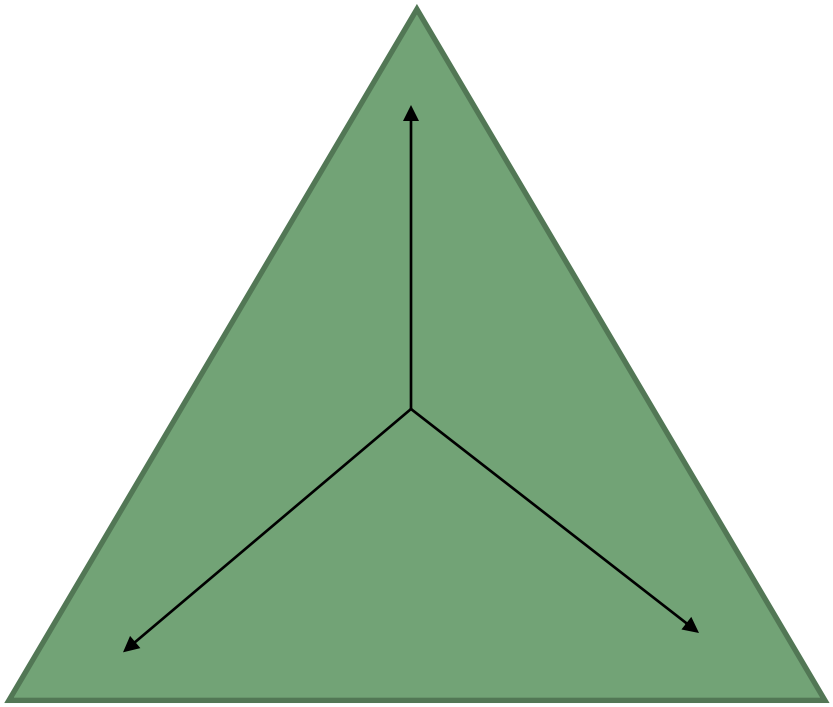
# Cân bằng An toàn và Truy cập Thông tin

Mọi người nên có một nút truy cập?

Thông tin có nên được giữ trong một kho bạc?

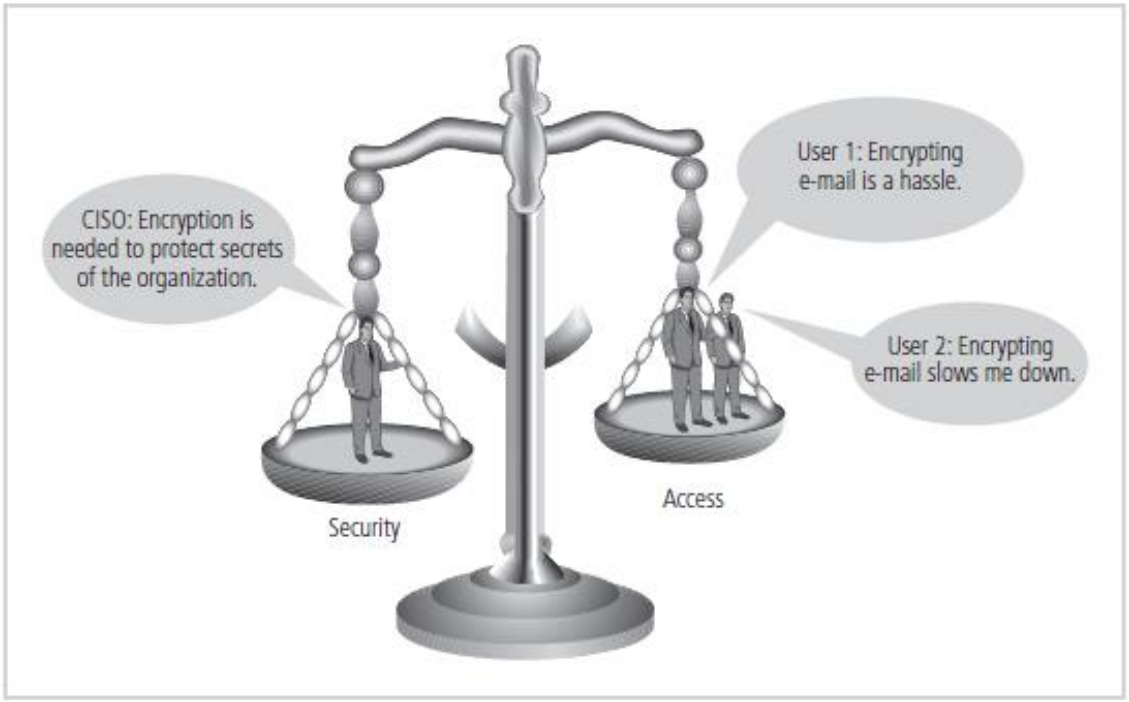
# Cân bằng An toàn và Truy cập Thông tin



# Cân bằng An toàn và Truy cập Thông tin

Không thể có được sự an toàn hoàn hảo — đó là một quá trình, không phải là một điều tuyệt đối

An toàn nên được coi là cân bằng giữa bảo vệ và tính khả dụng



# An toàn là nghệ thuật

Không có quy tắc cứng và nhanh hoặc nhiều giải pháp hoàn chỉnh được chấp nhận rộng rãi

Không có hướng dẫn sử dụng để triển khai bảo mật thông qua toàn bộ hệ thống

# An toàn là khoa học

Xử lý công nghệ được thiết kế để hoạt động ở mức hiệu suất cao

Các điều kiện cụ thể gây ra hầu như tất cả các hành động xảy ra trong hệ thống máy tính

Gần như mọi lỗi, lỗ hổng bảo mật và trục trặc hệ thống đều là kết quả của sự tương tác giữa phần cứng và phần mềm cụ thể

Nếu các nhà phát triển có đủ thời gian, họ có thể giải quyết và loại bỏ các lỗi

# Nguyên tắc quản lý an toàn thông tin

Các đặc điểm sau sẽ là trọng tâm của khóa học hiện tại (sáu chữ P):

1. Lập kế hoạch
2. Chính sách
3. Các chương trình
4. Sự bảo vệ
5. Con người
6. Quản lý dự án

1.**Planning**

2.**Policy**

3.**Programs**

4.**Protection**

5.**People**

6.**Project Management**

http://csrc.nist.gov/publications/PubsTC.html

# Lập kế hoạch

- Lập kế hoạch như một phần của quản lý InfoSec
  - Phần mở rộng của mô hình kế hoạch cơ sở đã được thảo luận trước đó
- Có trong mô hình lập kế hoạch InfoSec
  - Các hoạt động cần thiết để hỗ trợ thiết kế, tạo và thực hiện các chiến lược an toàn thông tin

# Lập kế hoạch (tiếp theo)

**Các loại kế hoạch InfoSec**

- Lập kế hoạch ứng phó sự cố
- Kế hoạch kinh doanh liên tục
- Lập kế hoạch khắc phục hậu quả thiên tai
- Hoạch định chính sách
- Kế hoạch nhân sự
- Lập kế hoạch triển khai công nghệ
- Lập kế hoạch quản lý rủi ro
- Lập kế hoạch chương trình an toàn
  - bao gồm giáo dục, đào tạo và nhận thức

# Chính sách

- Tập hợp các hướng dẫn tổ chức quy định hành vi nhất định trong tổ chức

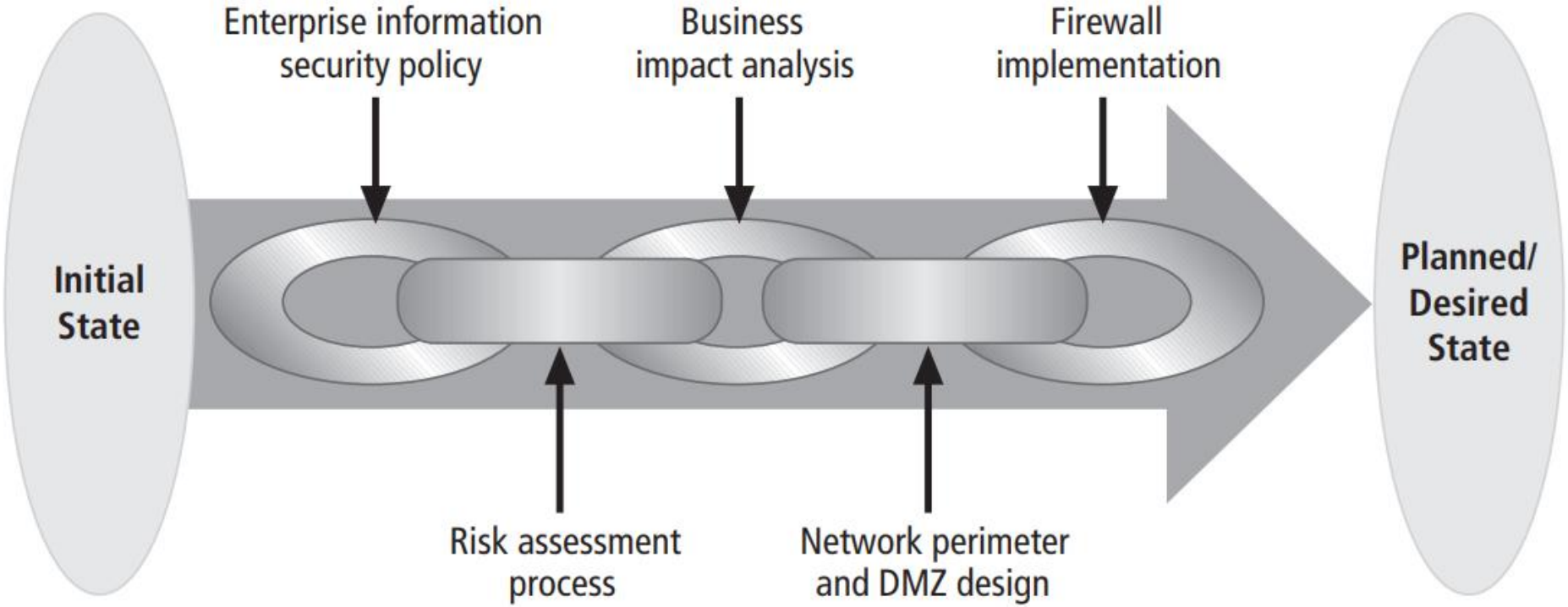
- **Ba loại chính sách chung:**
  - Chính sách bảo mật thông tin doanh nghiệp (EISP)
  - Chính sách bảo mật theo vấn đề cụ thể (ISSP)
  - Các chính sách dành riêng cho hệ thống (SysSP)

# Các chương trình

- Các hoạt động InfoSec được quản lý cụ thể như các thực thể riêng biệt
  - Ví dụ: chương trình đào tạo và nâng cao nhận thức về an toàn

- Các loại chương trình khác
  - Chương trình An ninh vật lý
    - xử lý với hỏa hoạn, truy cập vật lý, cổng, bảo vệ, v.v.

# Các chương trình




Một chuỗi chương trình an toàn thông tin

# Sự bảo vệ

- Thực hiện thông qua các **hoạt động quản lý rủi ro**

  Bao gồm:
  - Đánh giá và kiểm soát rủi ro
  - Cơ chế bảo vệ
  - Công nghệ
  - Công cụ

- Mỗi cơ chế thể hiện một số khía cạnh của việc quản lý các biện pháp kiểm soát cụ thể trong kế hoạch an toàn thông tin tổng thể

# Con người

Các nhà quản lý phải nhận ra vai trò quan trọng của mọi người trong chương trình an toàn thông tin

Khu vực này của InfoSec bao gồm nhân viên đảm bảo an ninh và an toàn của nhân viên, cũng như các khía cạnh của chương trình giáo dục nhận thức về ATTT

**Liên kết quan trọng nhất trong chương trình bảo mật thông tin**

# Quản lý dự án

Xác định và kiểm soát các nguồn lực được áp dụng cho dự án

Đo lường tiến độ

Điều chỉnh quy trình khi đạt được tiến độ

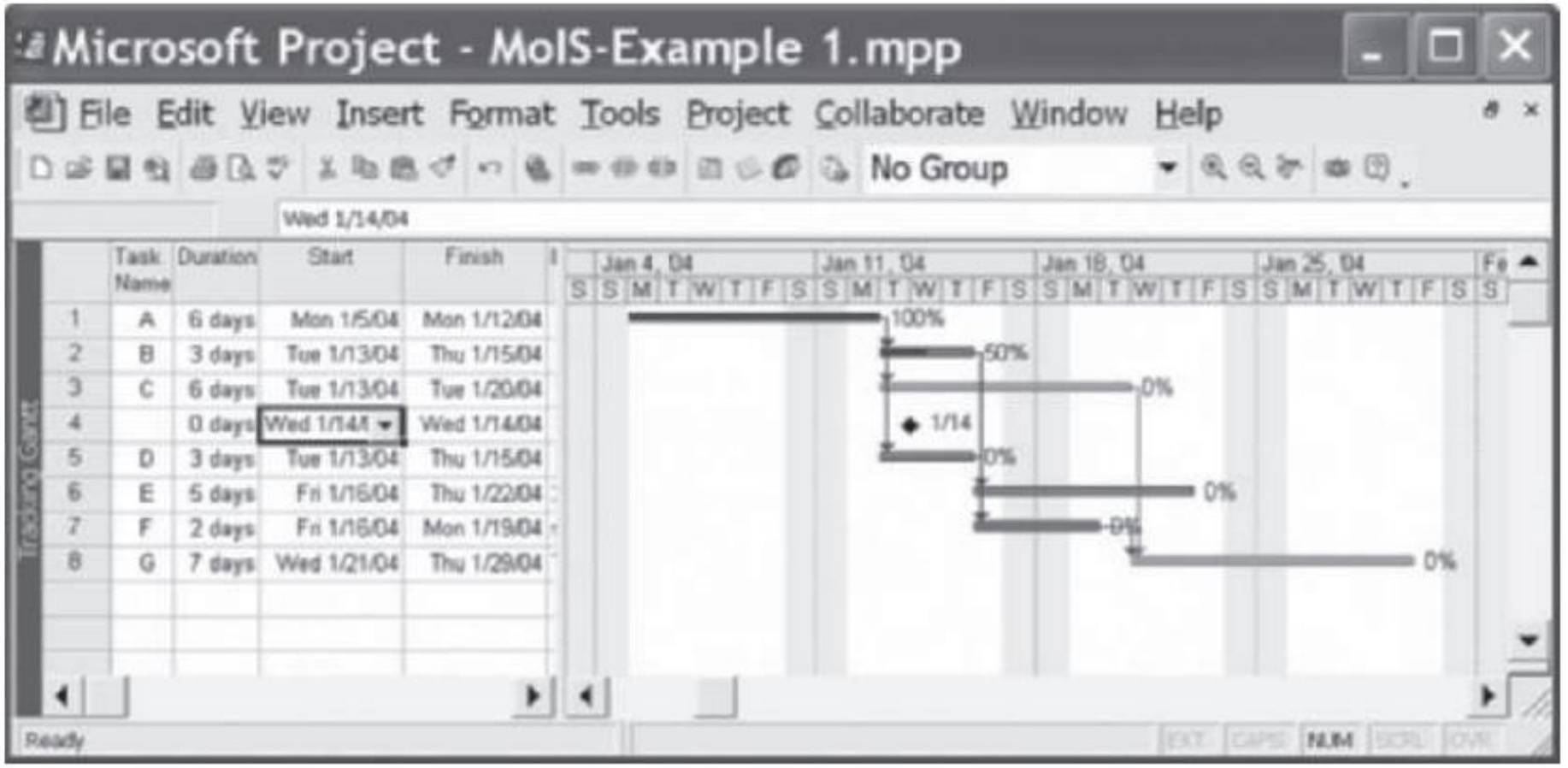
# Quản lý dự án

Ví dụ sơ lược về 1 cấu trúc phân rã công việc WBS

| Task | Effort (hours) | Skill | Dependencies |
|---|---|---|---|
| 1. Contact field office and confirm network assumptions | 2 | Network architect | |
| 2. Purchase standard firewall hardware | 4 | Network architect and purchasing group | 1 |
| 3. Configure firewall | 8 | Network architect | 2 |
| 4. Package and ship firewall to field office | 2 | Intern | 3 |
| 5. Work with local technical resource to install and test firewall | 6 | Network architect | 4 |
| 6. Complete network vulnerability assessment | 12 | Network architect and penetration test team | 5 |
| 7. Get remote office sign-off and update network drawings and documentation | 8 | Network architect | 6 |

# Quản lý dự án

Ví dụ về Gantt chart



# Tóm lược

- An toàn là gì?
- Nguyên tắc quản lý an toàn thông tin
  - Lập kế hoạch
  - Chính sách
  - Các chương trình
  - Sự bảo vệ
  - Con người
  - Quản lý dự án

# Bài tiếp theo

**Phần 2 - Lập kế hoạch ATTT**

# Closing case

# Review Questions

1. List and describe the three communities of interest that engage in an organization's efforts to solve InfoSec problems. Give two or three examples of who might be in each community.
2. What is information security? What essential protections must be in place to protect information systems from danger?
3. What is the importance of the C.I.A. triangle? Define each of its components.
4. Describe the CNSS security model. What are its three dimensions?
5. What is the definition of "privacy" as it relates to InfoSec? How is this definition different from the everyday definition? Why is this difference significant?
6. Define the InfoSec processes of identification, authentication, authorization, and accountability.
7. What is management and what is a manager? What roles do managers play as they execute their responsibilities?
8. How are leadership and management similar? How are they different?
9. What are the characteristics of management based on the method described in the text as the "popular approach" to management? Define each characteristic.
10. What are the three types of general planning? Define each.

11. List and describe the five steps of the general problem-solving process.
12. Define "project management." Why is project management of particular interest in the field of InfoSec?
13. Why are project management skills important to the InfoSec professional?
14. How can security be both a project and a process?
15. What are the nine areas that make up the component processes of project management?
16. What are the three planning parameters that can be adjusted when a project is not being executed according to plan?
17. Name and very briefly describe some of the manual and automated tools that can be used to help manage projects.
18. What is a work breakdown structure (WBS) and why is it important?
19. List and describe the various approaches to task sequencing.
20. How do PERT/CPM methods help to manage a project?