CHƯƠNG 02

TỔNG QUAN VỀ QUẢN LÍ RỦI RO AN TOÀN THÔNG TIN

10/2/2021

ThS.Nguyễn Duy
duyn@uit.edu.vn

Nội Dung

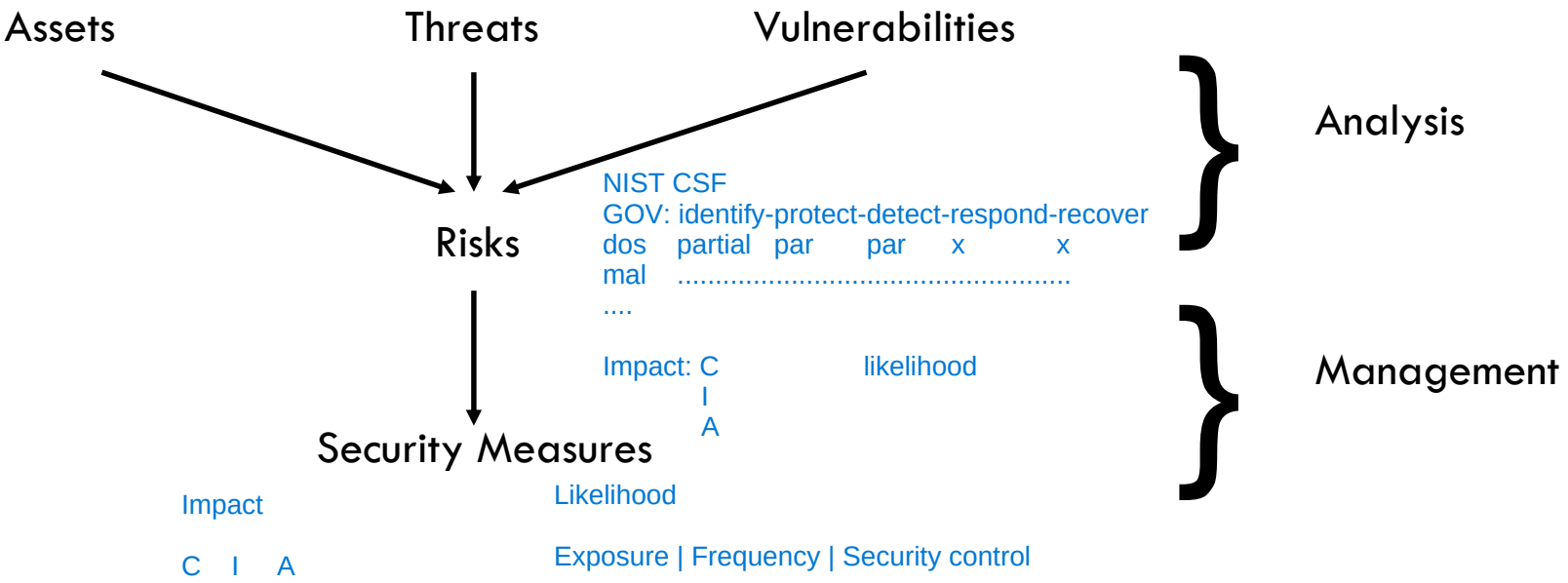
- Rủi ro là gì?
- Đánh giá rủi ro trong ATTT là gì?
- Qui trình đánh giá rủi ro trong ATTT?
- Qui trình quản lý rủi ro trong ATTT?

Nội Dung

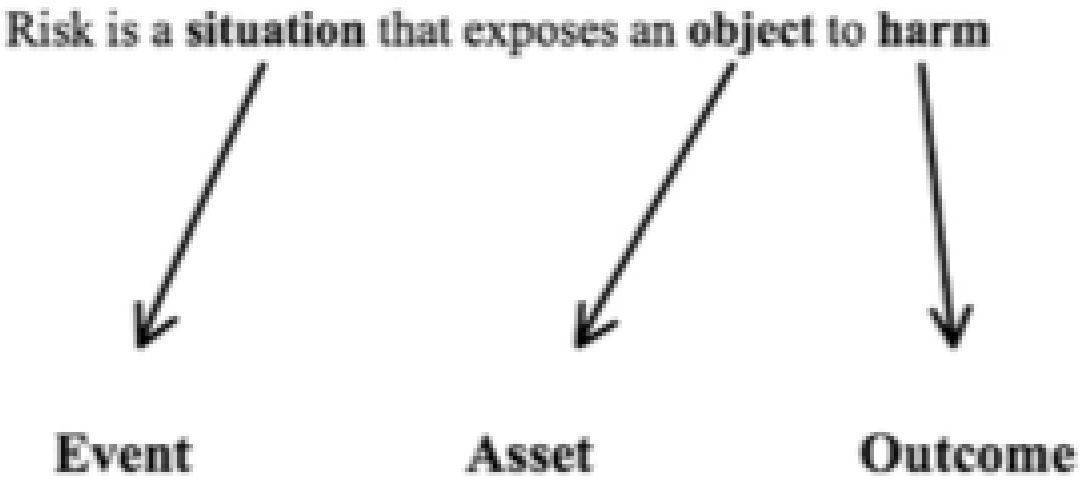
- **Rủi ro là gì?**
- Đánh giá rủi ro trong ATTT là gì?
- Qui trình đánh giá rủi ro trong ATTT?
- Qui trình quản lý rủi ro trong ATTT?

Rủi ro là gì?
Khái niệm

- A probability or threat of damage, injury, liability, loss, or any other negative occurrence that is caused by external or internal vulnerabilities.

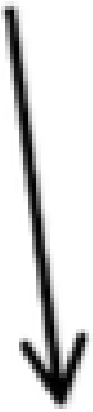


Rủi ro là gì?
Các thành phần trong Risk



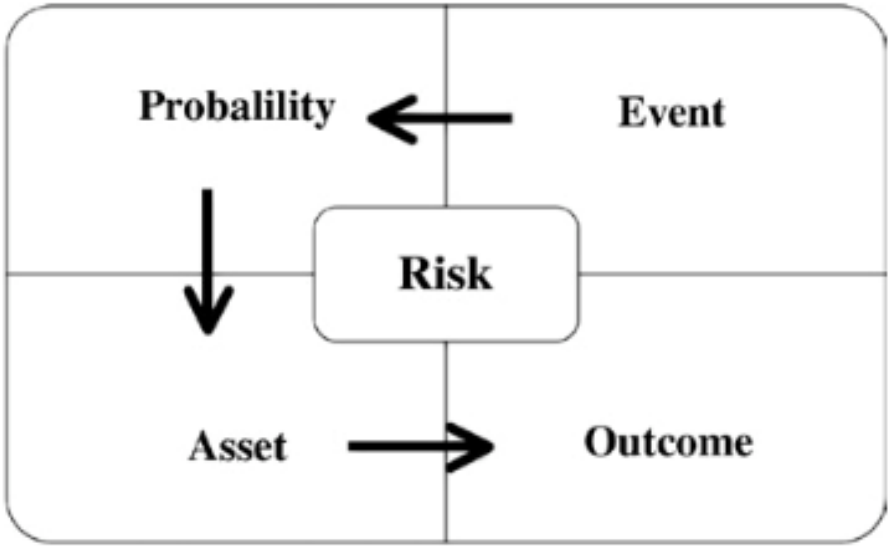
Rủi ro là gì?
Các thành phần trong Risk (Cont.)

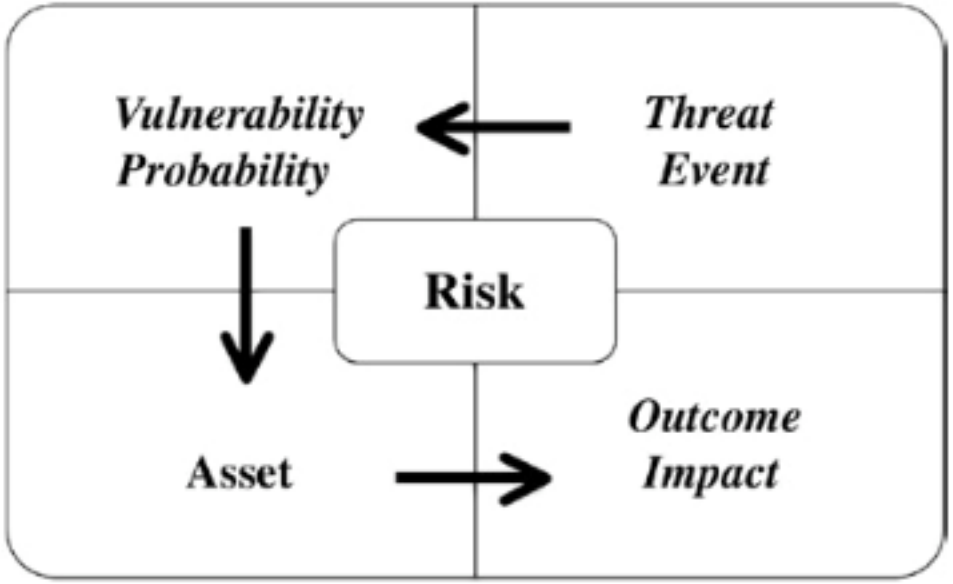
Risk is the **measurement** of uncertainty.



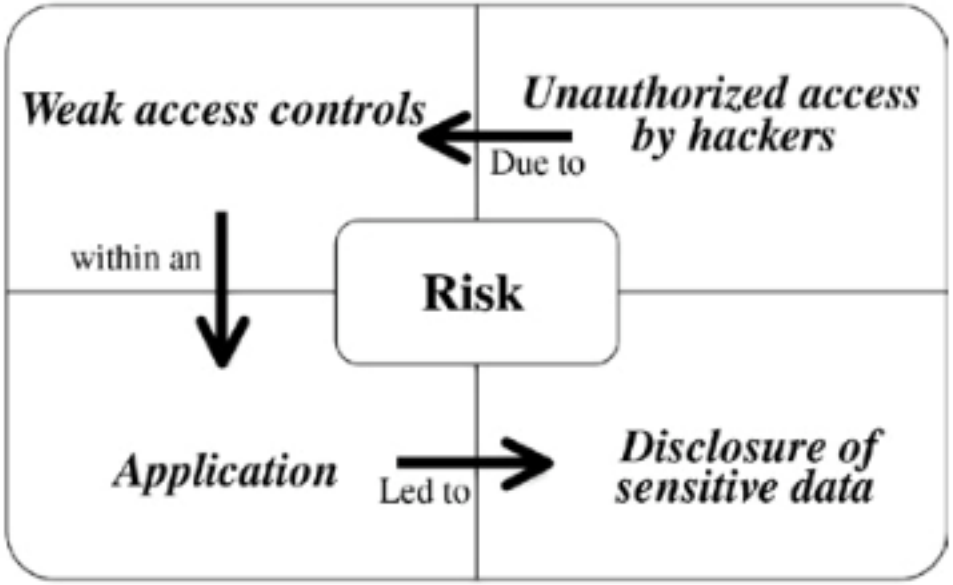
Probability

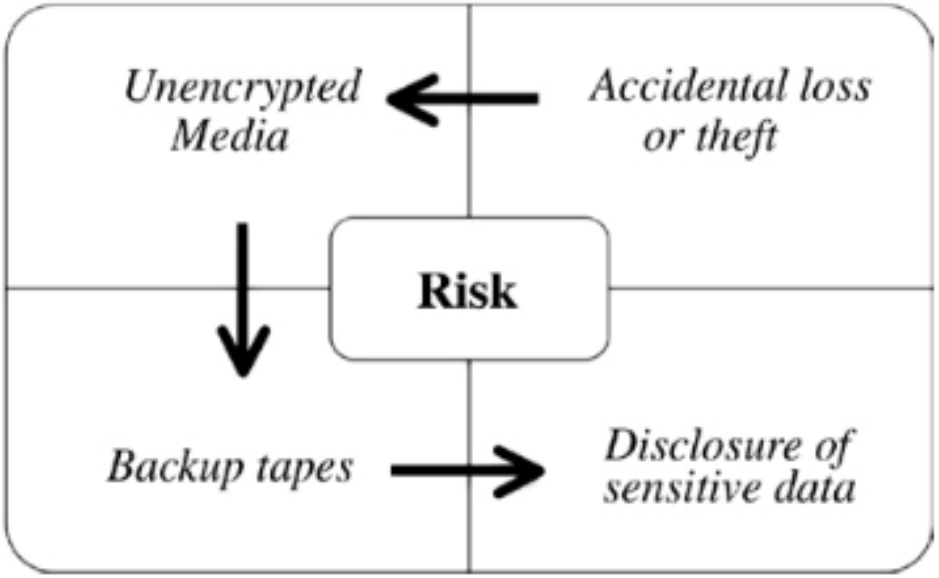
Rủi ro là gì?
Sự tương tác giữa các thành phần





Rủi ro là gì?
Sự tương tác giữa các thành phần





Nội Dung

- Rủi ro là gì?
- **Đánh giá rủi ro trong ATTT là gì?**
- Qui trình đánh giá rủi ro trong ATTT?
- Qui trình quản lý rủi ro trong ATTT?

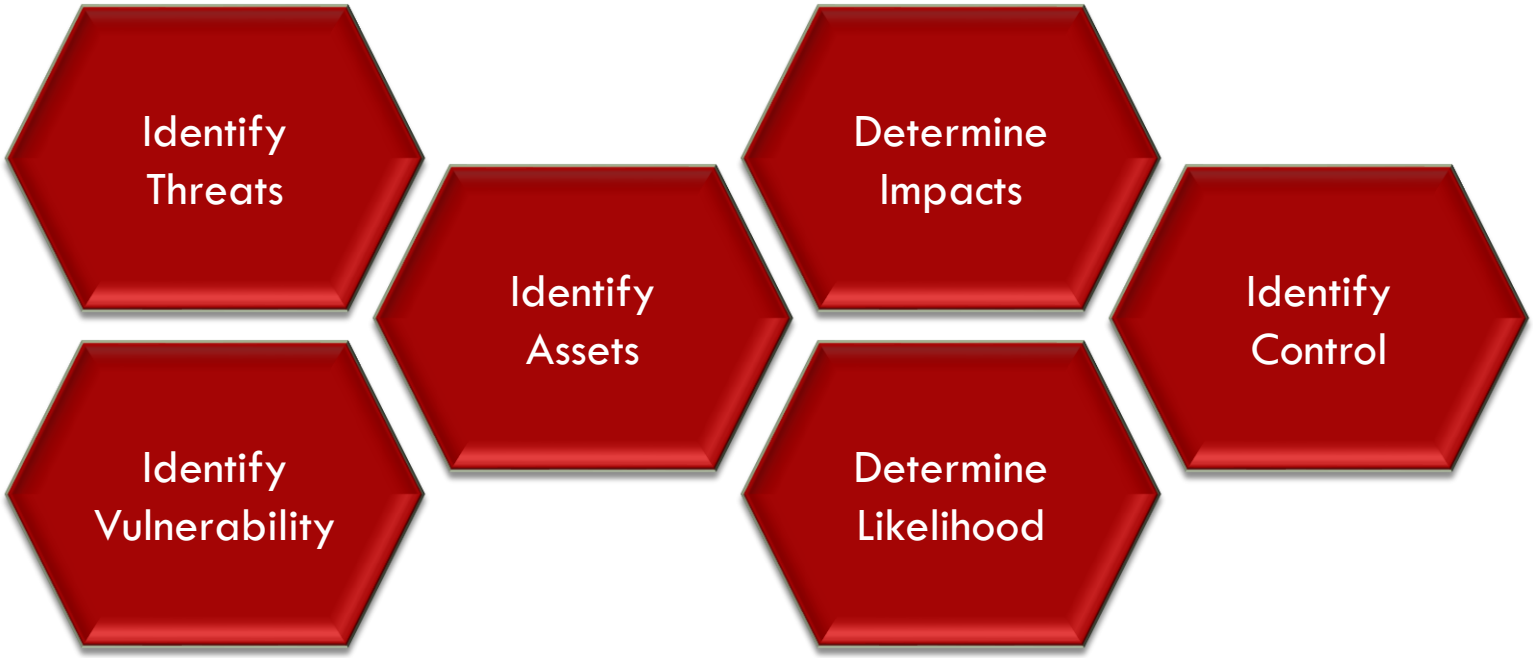
Đánh giá rủi ro trong ATTT

Tại sao cần?

- Xác định những tài sản nào cần bảo vệ
- Xác định mức độ rủi ro của các loại tài sản
- Xác định phương pháp bảo vệ tài sản
- Xác định nguồn lực cần bảo vệ tài sản
- Xác định ngân sách để triển khai chương trình bảo mật (security program).

Đánh giá rủi ro trong ATTT
Những công việc quan trọng

duyn@uit.edu.vn

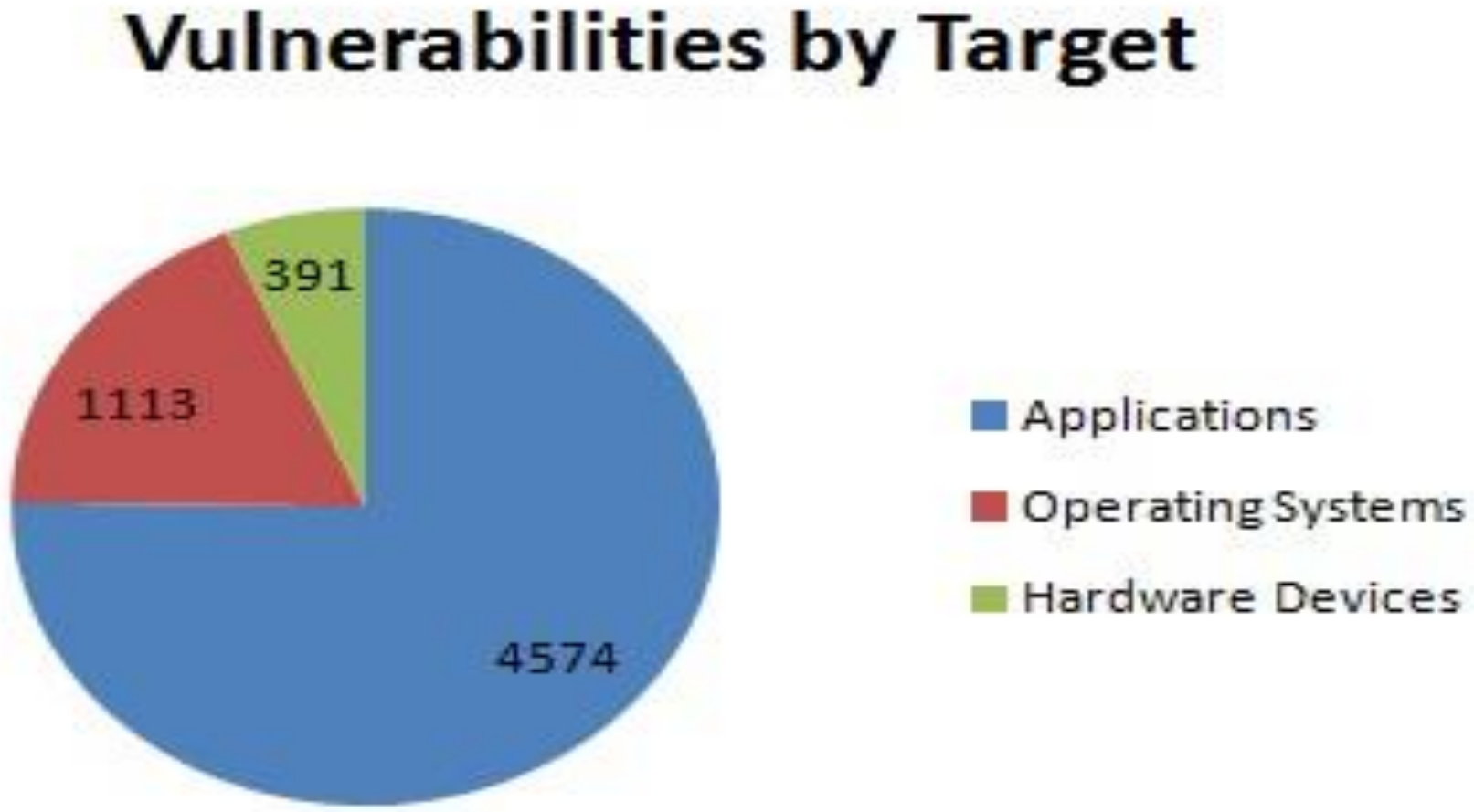


Đánh giá rủi ro trong ATTT
Xác định tài sản

- Database
- Application
- Hardware
- Software
- Processes
- People
- impact is the outcome, typically harmful, of a threat applied to an asset.

Đánh giá rủi ro trong ATTT

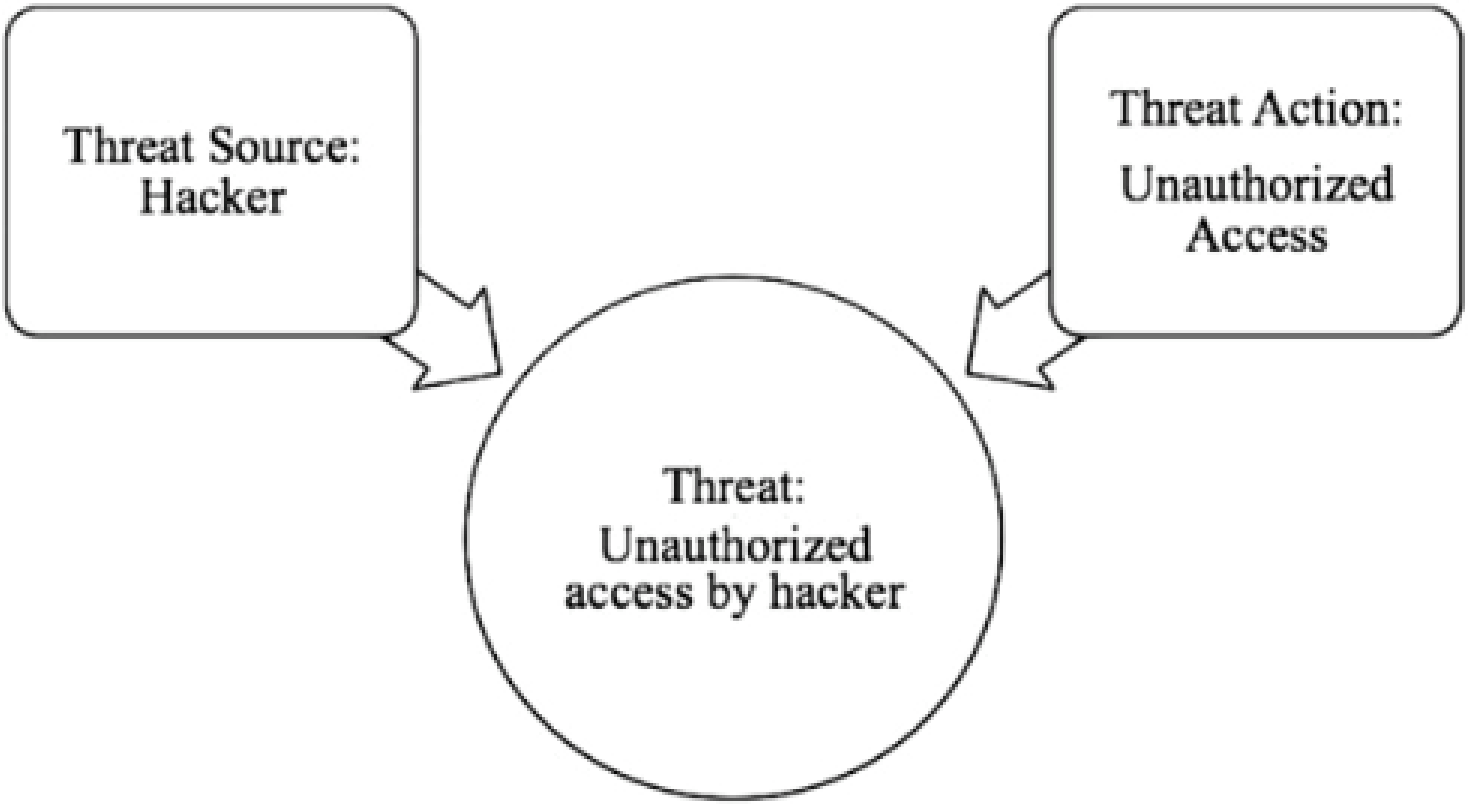
Xác định lỗ hổng



Đánh giá rủi ro trong ATTT

Xác định mối đe doạ

use threat model
STRIDE



Đánh giá rủi ro trong ATTT
Khai thác lỗ hổng

Đánh giá rủi ro trong ATTT
Xác định tác động

- *Impact is the outcome, typically harmful, of a threat applied to an asset.*

Đánh giá rủi ro trong ATTT
Determine likelihood

- *Likelihood is the probability that a threat would exploit a vulnerability to affect an asset*

Đánh giá rủi ro trong ATTT
Xác định cơ chế kiểm soát

- *Controls are mechanisms that detect or prevent threats sources from leveraging vulnerabilities and thus are closely tied to likelihood as it affects the probability of a risk*

Mục tiêu đánh giá rủi ro trong ATTT

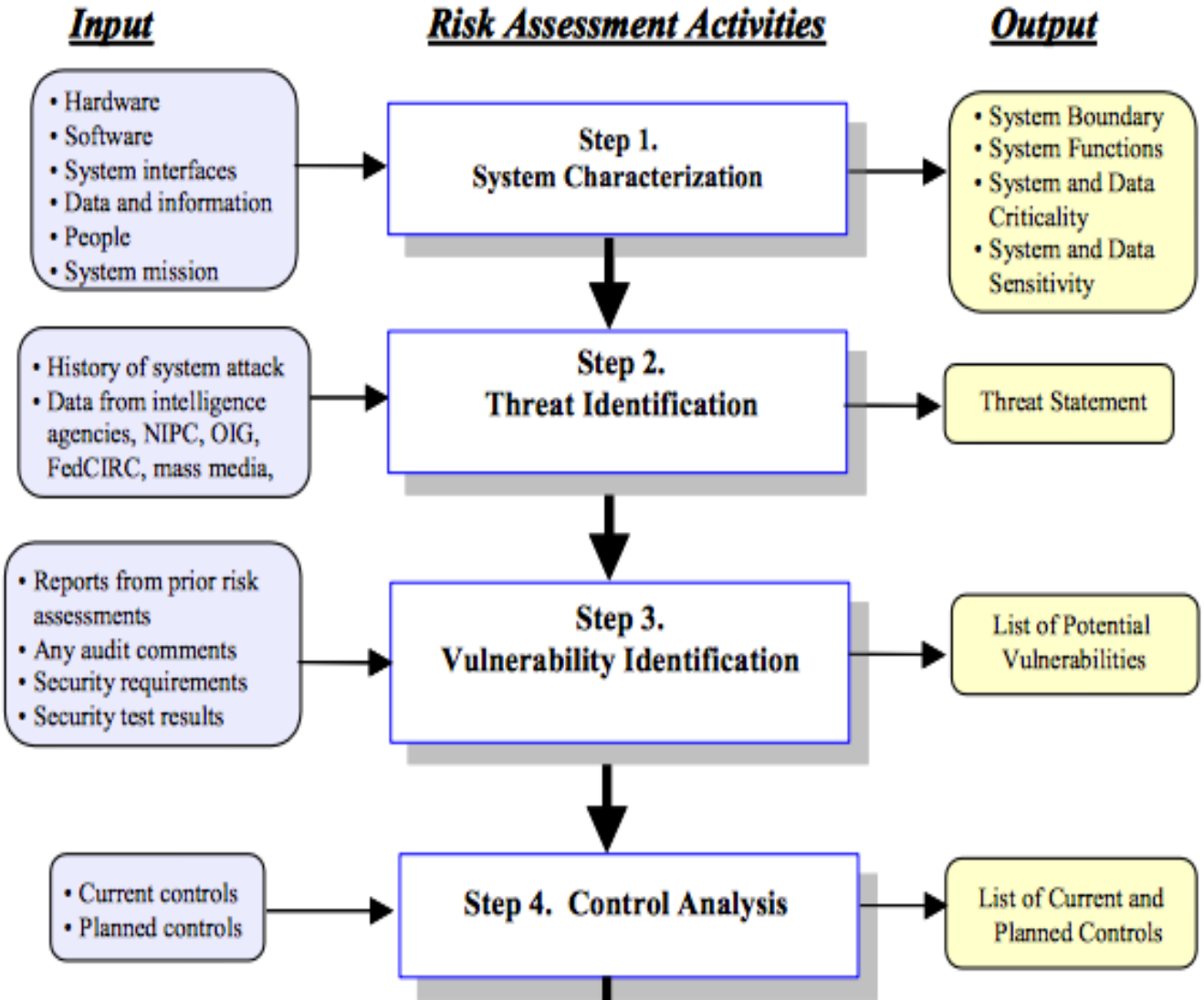
- “The process of identifying the risks to system security and determining the probability of occurrence, the resulting impact, and additional safeguards that would mitigate this impact.”

Nội Dung

- Rủi ro là gì?
- Đánh giá rủi ro trong ATTT là gì?
- **Qui trình đánh giá rủi ro trong ATTT?**
- Qui trình quản lý rủi ro trong ATTT?

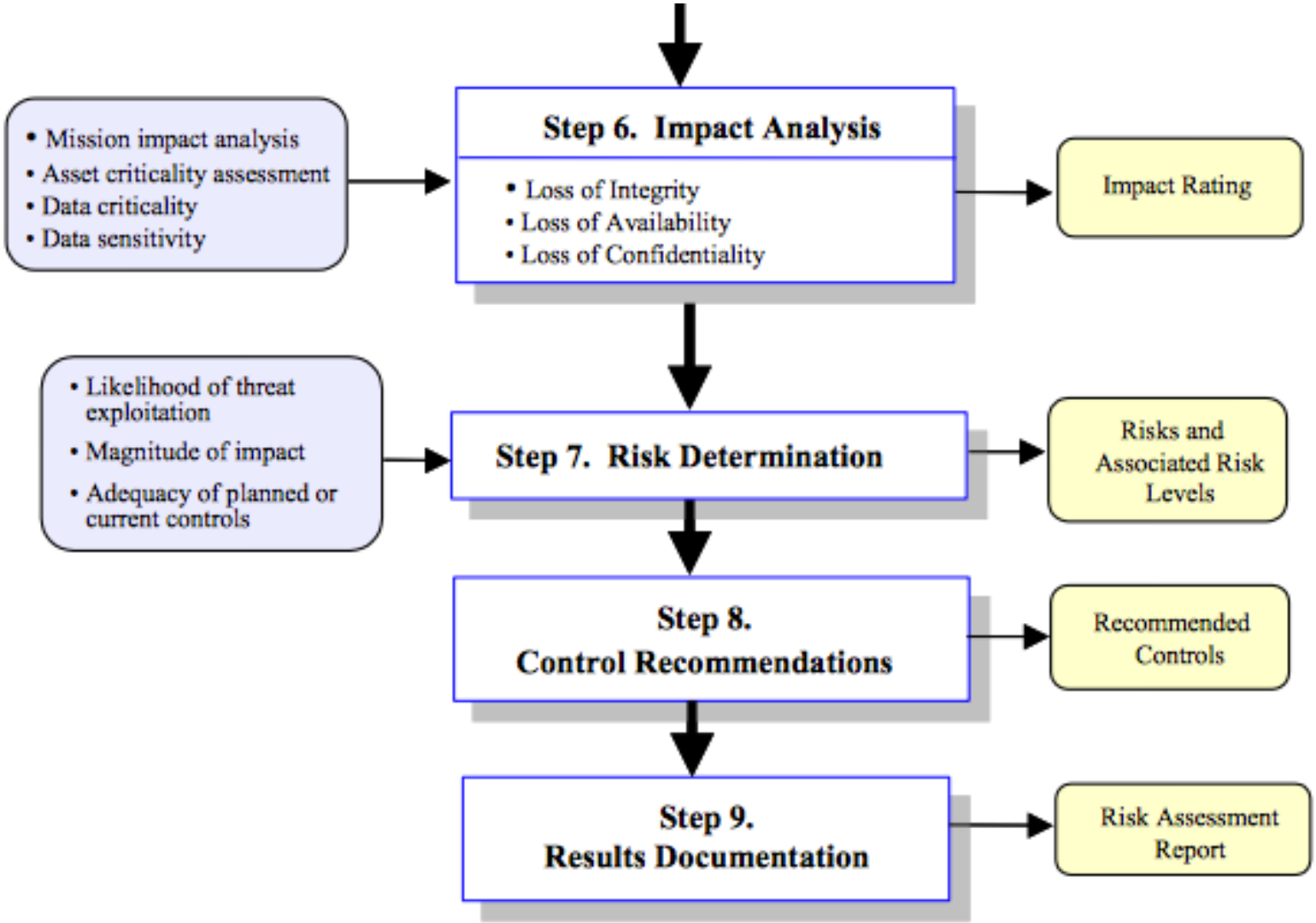
Phương pháp đánh giá rủi ro trong ATTT

duyn@uit.edu.vn

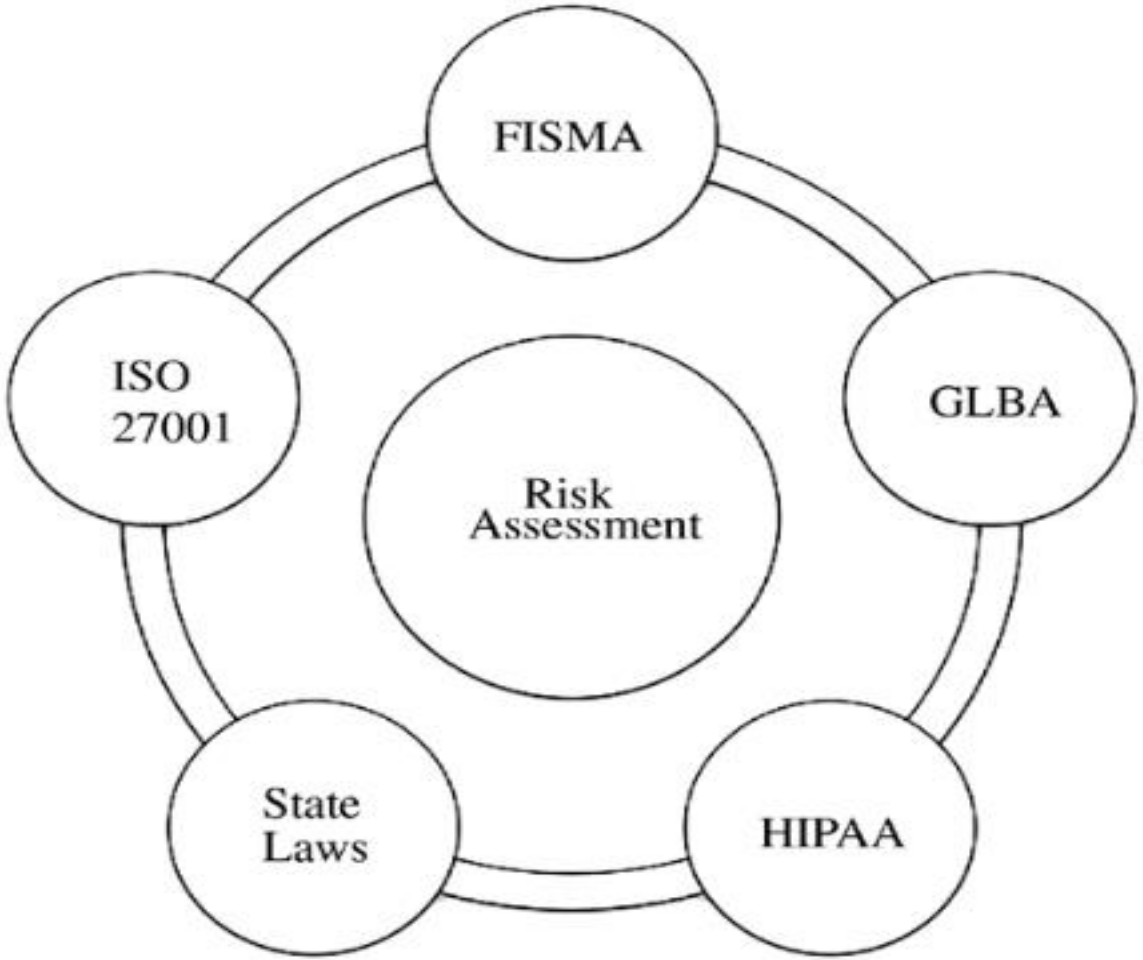


Phương pháp đánh giá rủi ro trong ATTT

duyn@uit.edu.vn

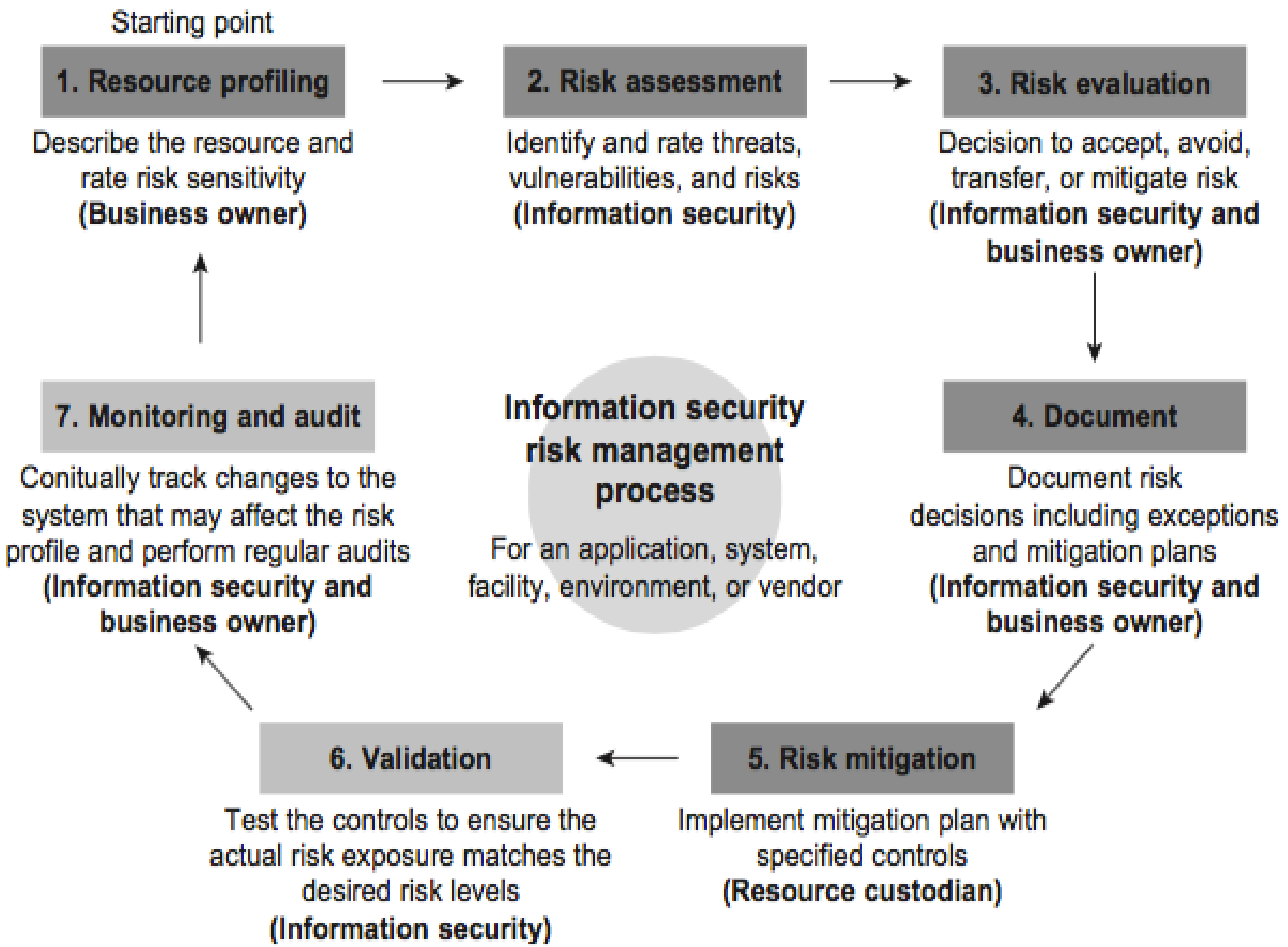


Drivers (trình điều khiển), Laws (luật), và Regulations (qui tắc)



Nội Dung

- Rủi ro là gì?
- Đánh giá rủi ro là gỉ?
- Qui trình đánh giá rủi ro ATTT?
- **Qui trình quản lý rủi ro ATTT?**


Starting point
1. Resource profiling
Describe the resource and rate risk sensitivity (Business owner)
2. Risk assessment
Identify and rate threats, vulnerabilities, and risks (Information security)
3. Risk evaluation
Decision to accept, avoid, transfer, or mitigate risk (Information security and business owner)
4. Document
Document risk decisions including exceptions and mitigation plans (Information security and business owner)
5. Risk mitigation
Implement mitigation plan with specified controls (Resource custodian)
6. Validation
Test the controls to ensure the actual risk exposure matches the desired risk levels (Information security)
7. Monitoring and audit
Conitually track changes to the system that may affect the risk profile and perform regular audits (Information security and business owner)
Information security risk management process
For an application, system, facility, environment, or vendor