Risk Management

Introduction
Chapter 1

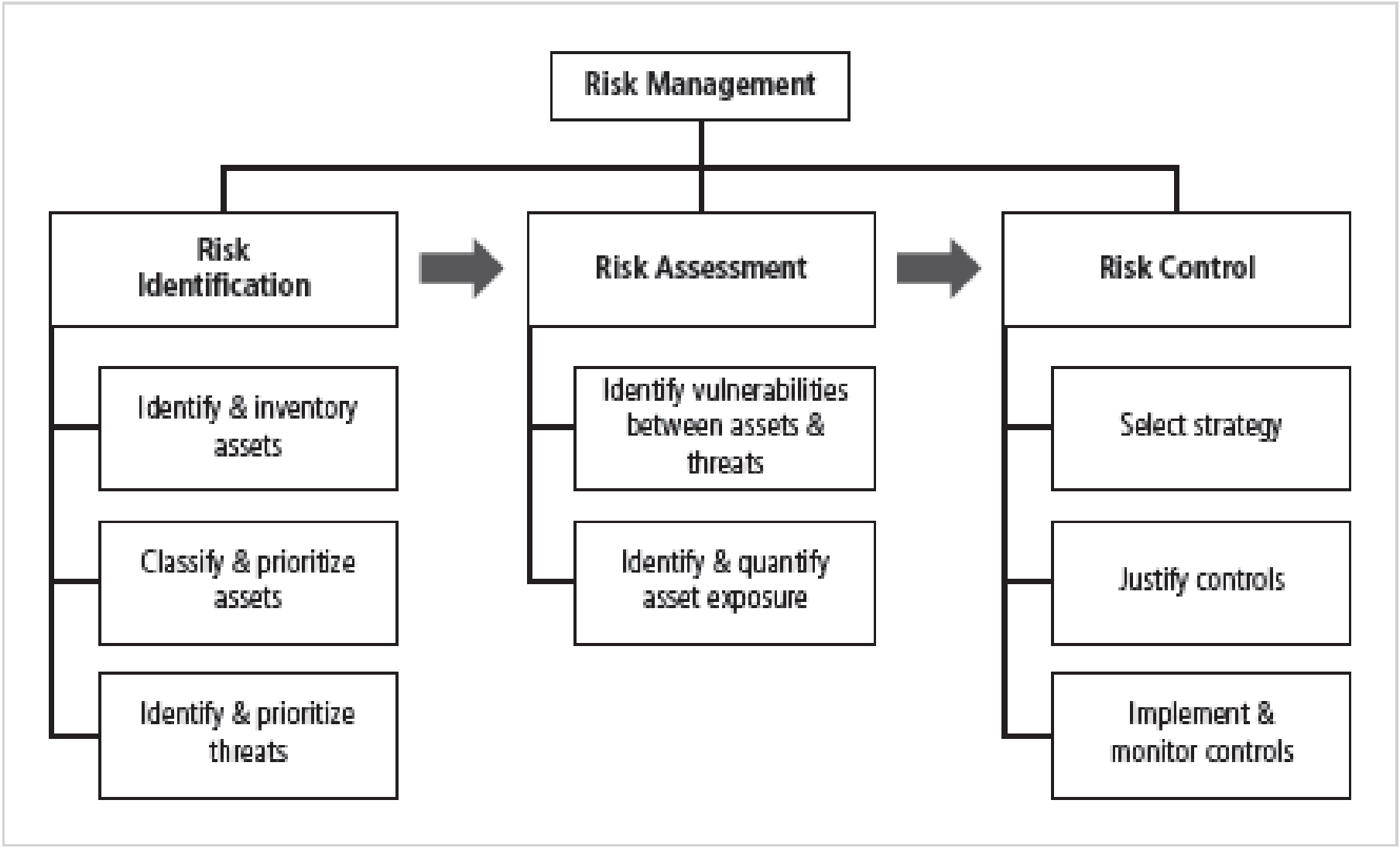
أ.م.د.عباس عبد العزيز عبد الحميد

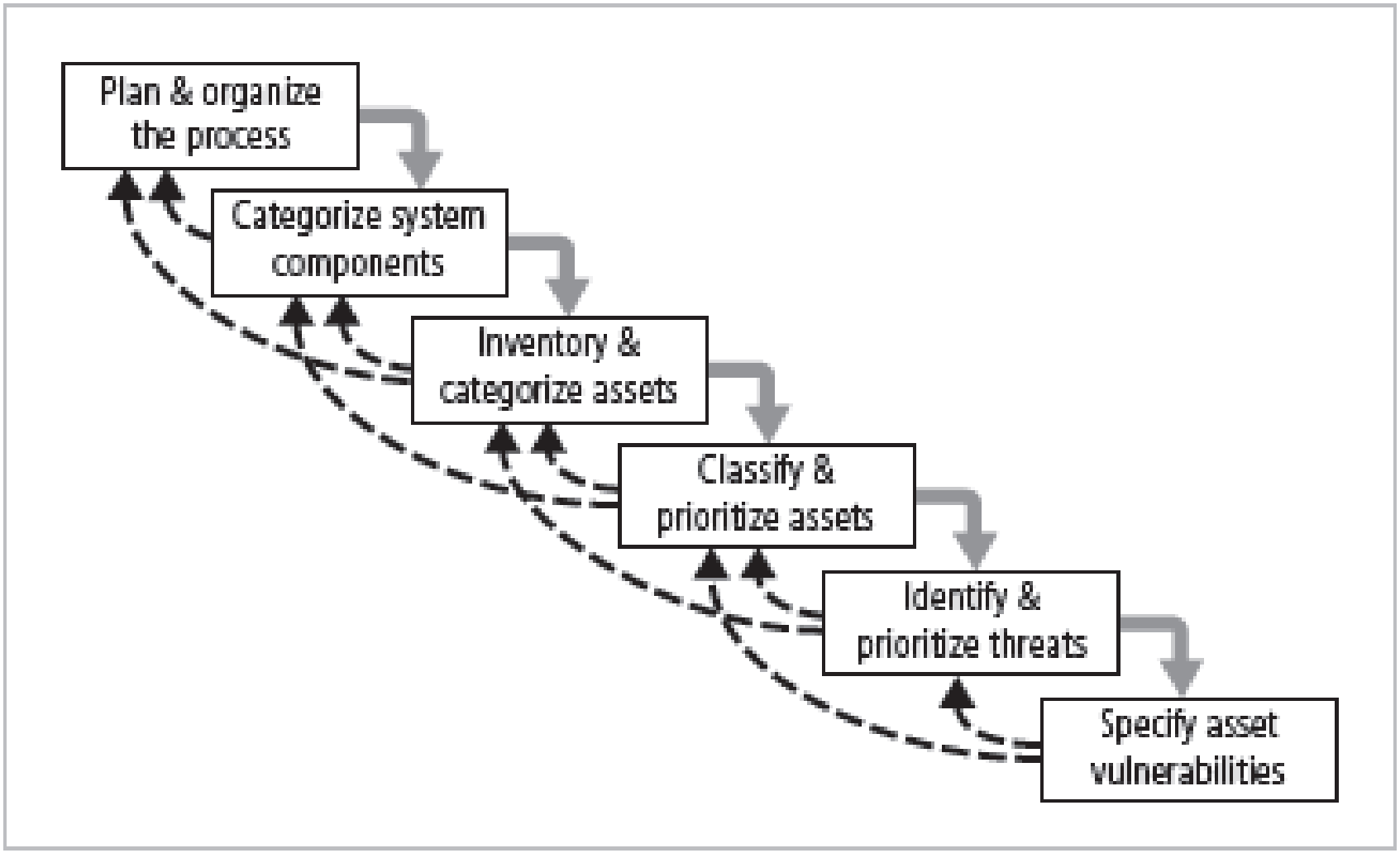
كليـة العلـوم / قسم الحاسـوب

abbasabdulazeez@uomustansiriyah.edu.iq

Risk Identification

- Assets are targets of various threats and threat agents.
- Risk management process of identifying and controlling risks facing an organization.
- Risk identification begins with identifying organization's assets and assessing their value


Risk Management
Risk Identification
Identify & inventory assets
Classify & prioritize assets
Identify & prioritize threats
Risk Assessment
Identify vulnerabilities between assets & threats
Identify & quantify asset exposure
Risk Control
Select strategy
Justify controls
Implement & monitor controls


Plan & organize the process
Categorize system components
Inventory & categorize assets
Classify & prioritize assets
Identify & prioritize threats
Specify asset vulnerabilities

What is Cybersecurity Risk Management?

- Cybersecurity risk management is the continuous process of identifying, analyzing, evaluating, and addressing an organization's cyber security threats. Learn how to design and implement your security processes.
- Cybersecurity Risk Management must be continuous in order to maintain protections. Other factors beyond the changing threat landscape also affect existing cybersecurity risk planning.
- Regulations are often changed, or new ones introduced.
- The risks associated with these changes need to be analyzed, and cybersecurity policies and procedures changed to ensure compliance.

What is Risk Management strategy?

implements the four quadrants that deliver comprehensive digital risk protection:

- Map - Discover and map all digital assets to quantify the attack surface. Use the map as a foundation to monitor cybercriminal activity.
- Monitor - Search the public and dark web for threat references to your digital assets. Translate found threats to actionable intelligence.
- Mitigate - Automated actions to block and remove identified threats to digital assets. Includes integration with other security initiatives in place.
- Manage - Manage the process used in Map, Manage, and Mitigate quadrants. Management is essential to successful digital risk protection.

What are the Benefits of Cybersecurity Risk Management?

Implementing Cybersecurity Risk Management ensures that cybersecurity is not relegated to an afterthought in the daily operations of an organization. Having a Cybersecurity Risk Management strategy in place ensures that procedures and policies are followed at set intervals,and security is kept up to date.

What are the Benefits of Cybersecurity Risk Management?

Cybersecurity Risk Management provides ongoing monitoring, identification, and mitigation of the following threats:

- Phishing Detection.
- VIP and Executive Protection.
- Brand Protection.
- Fraud Protection.
- Sensitive Data Leakage Monitoring.
- Dark Web Activity.
- Automated Threat Mitigation.
- Leaked Credentials Monitoring.
- Malicious Mobile App Identification.
- Supply Chain Risks.

The importance of risk management

Risk management is a key requirement of many information security standards and frameworks, and laws such as the

- GDPR (General Data Protection Regulation).

- NIS Regulations (Network and Information Systems Regulations 2018).

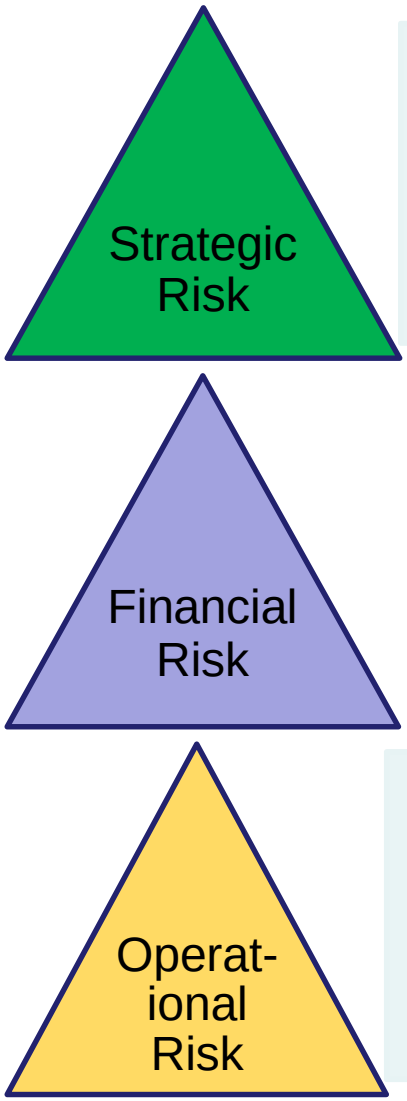
Standards and frameworks that mandate a cyber risk management approach

- ISO 31000 Risk Management:
  - **"Risk is the effect of uncertainty on objectives"**
  - No distinction between positive and negative effects of uncertainty
  - This definition is very general, and too abstract for IS risk assessment
  - But ISO 31000 also says: **Risk is often expressed as the combination of the *likelihood of occurrence of an event* and the associated *consequences of the event.***

- ISO 27005 (Information Security Risk)
  - **"Risk is the potential that a given threat will exploit vulnerabilities of assets and thereby cause harm to the organization."**

- Harris, CISSP 8th ed.:
  - **"Risk is the likelihood of a threat agent taking advantage of a vulnerability and the resulting business impact."** (Glossary p.1292)

Risk Categories

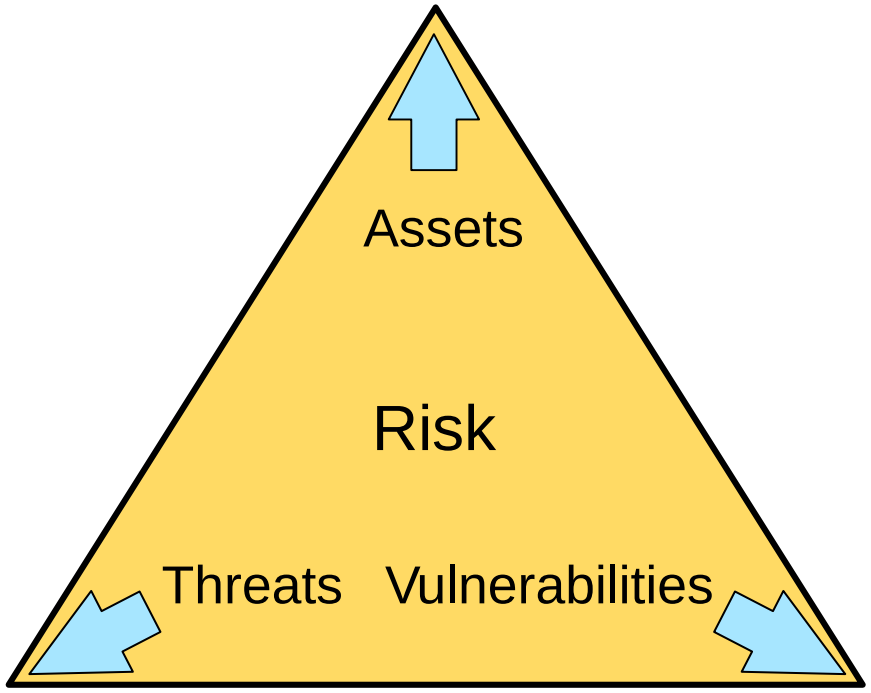


Risk related to long-term strategies and plans
- Disruptive technological development
- New Competitors in the market
- Changing laws, regulation and politics
- Unstable global economy

Risk related to the financial situation of the organisation
- Return on investments
- Sales and price levels in the market
- Cost of operations
- Liquidity

Risk related to events with negative impact on operations
- Accidents and failures
- Natural events (flood, fire)
- Intentional adversarial actions
- **Information security and cyber incidents**

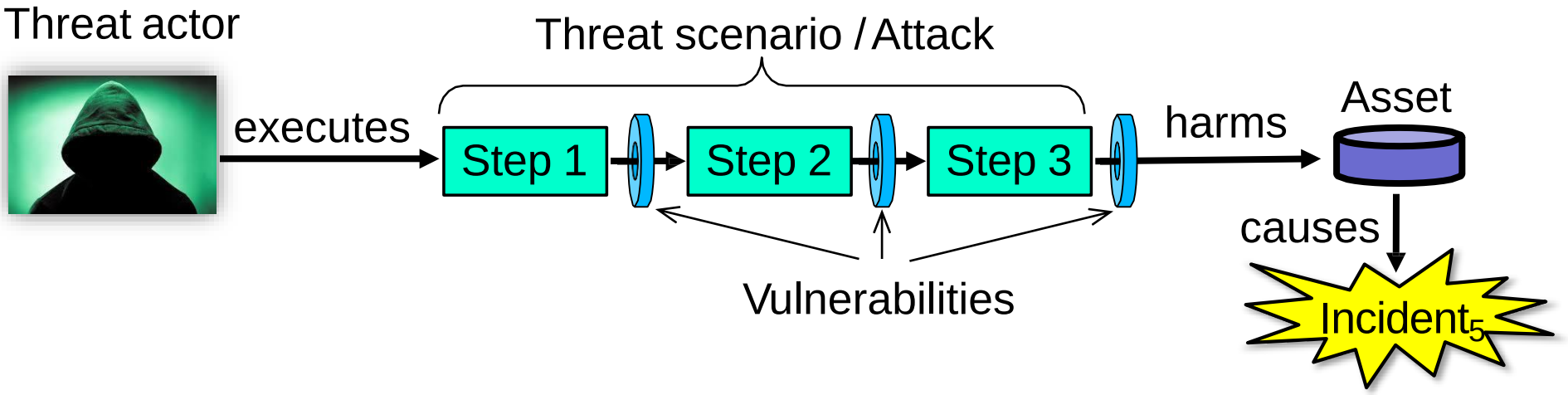
General IS Risk Model



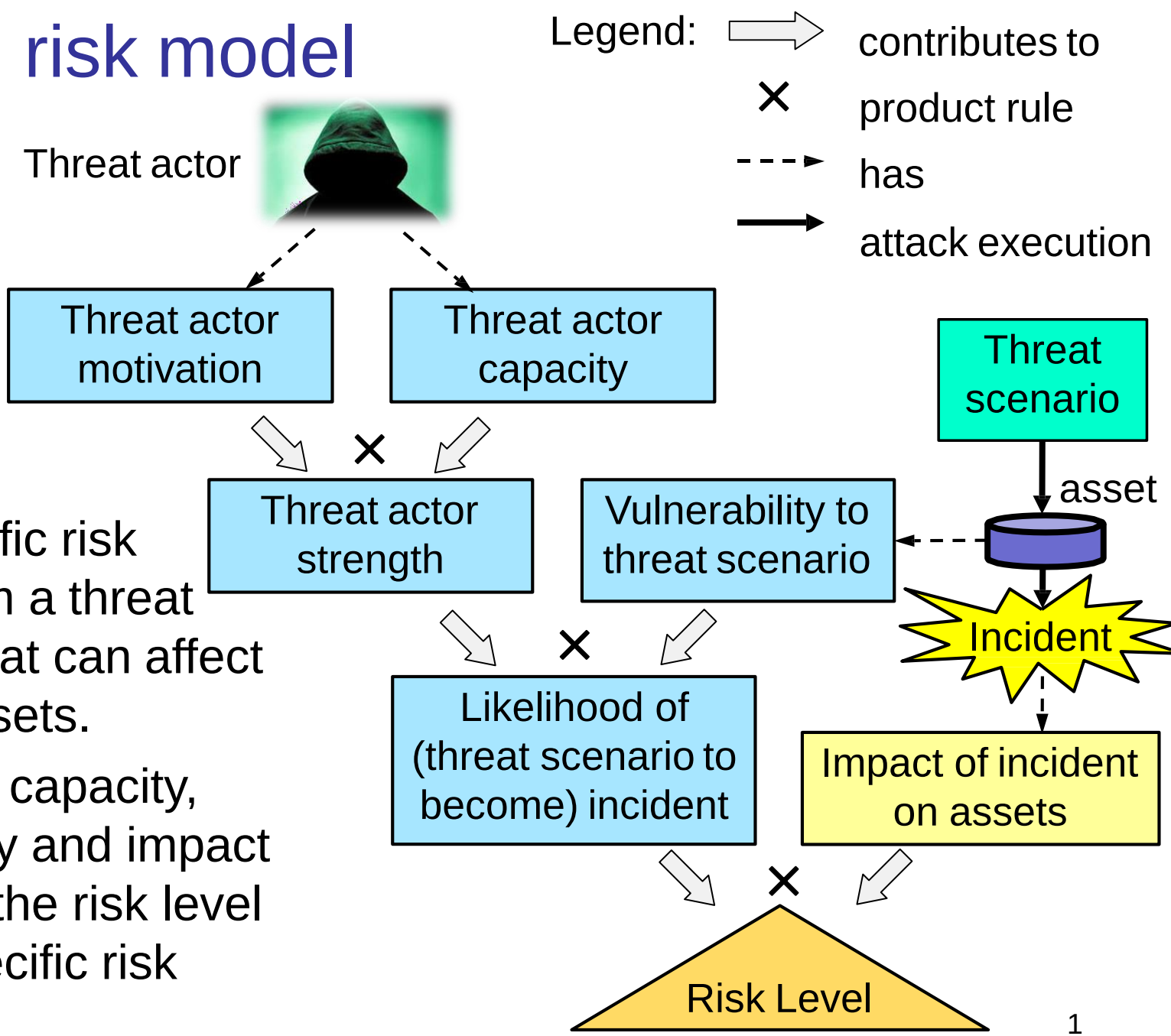
- General model for information-security risk
  - The more assets you have, the more threats you are exposed to, and the more vulnerable you are, then the greater the risk.

Threats and Vulnerabilities

- **Threat:** A scenario of steps, controlled by a threat actor, which can harm the victim's information assets.
- **Asset:** Something which is of value to the organization.
  - CIA and privacy of data, IT systems and services
- **Vulnerability:** Absence of security controls to stop threats.
- **Attack:** Execution of a threat
- **Incident:** Result of a (successful) attack

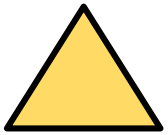


Detailed risk model



- Each specific risk results from a threat scenario that can affect specific assets.
- Motivation, capacity, vulnerability and impact determine the risk level for that specific risk

Identifying specific risks

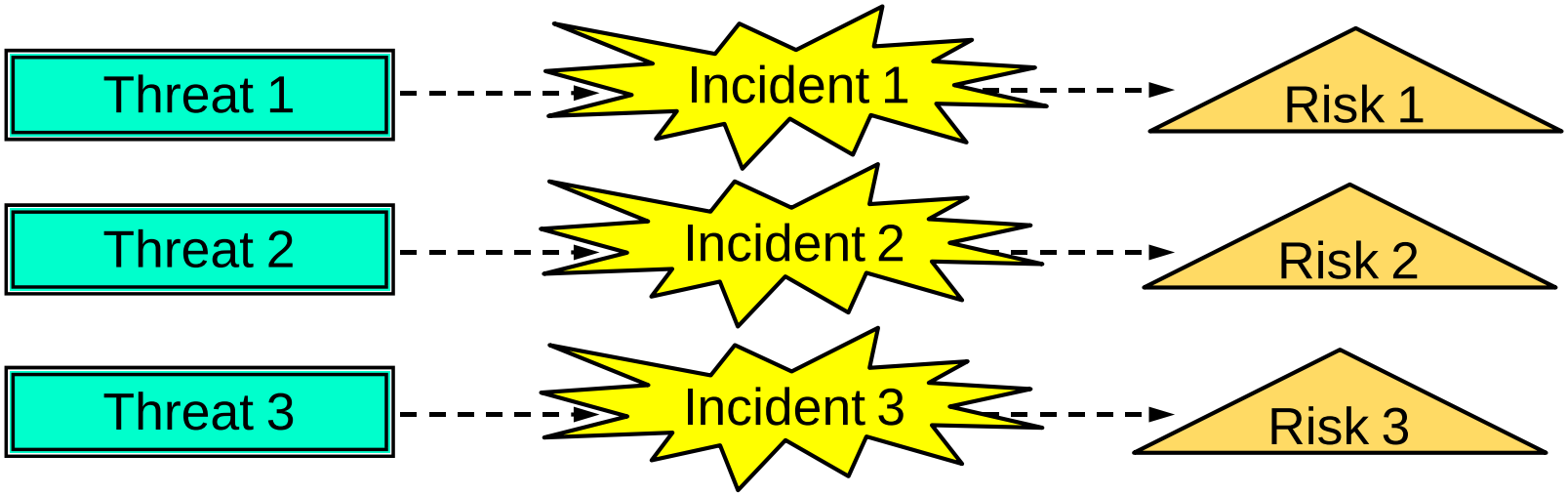


- The relevant combination of a threat scenario, vulnerabilities, and the resulting incident and impact represents a single specific risk
- All relevant specific risks should be identified

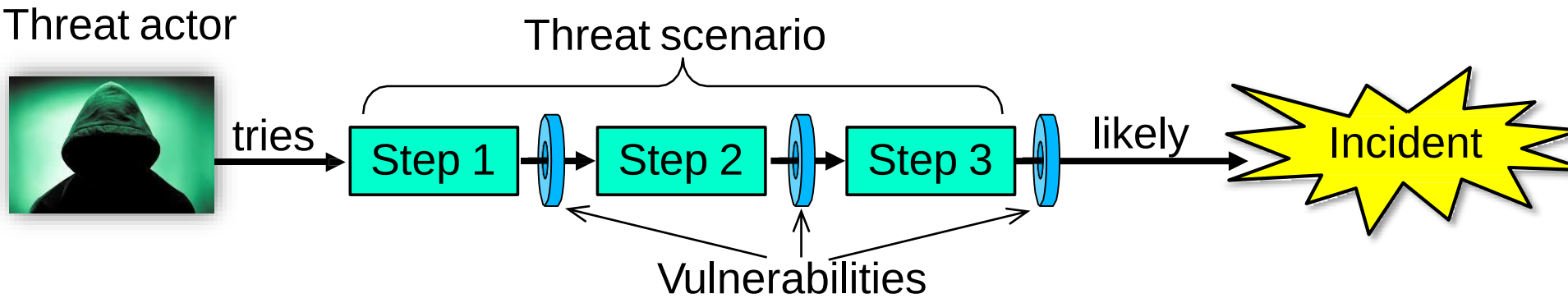
Threats / incidents	**Vulnerabilities**	**Asset impacts**
•Password compromise	•Weak passwords	•Deleted files
•SQL injection	•Poor awareness	•Stolen files
•Logical bomb in SW	•No input validation	•Corrupted files
•Trojan infects clients	•Outdated antivirus	•Intercepted traffic
•Cryptanalysis of cipher	•Weak ciphers	•False transaction
•Brute force attack	•Short crypto keys	•Process disruption
•Social engineering	•Poor usability	•Damaged reputation
• …..	• …	• …

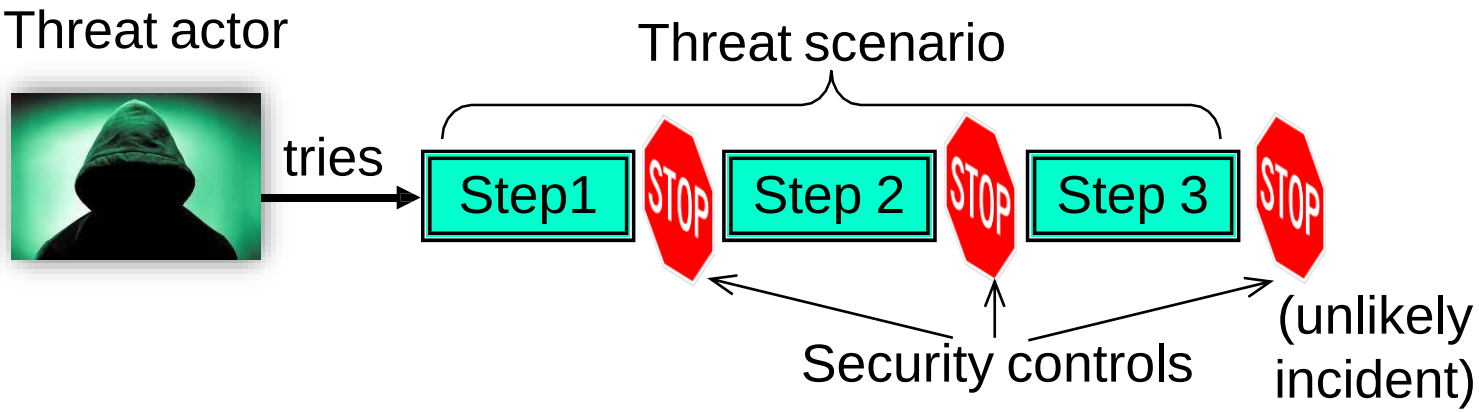
Many Risks

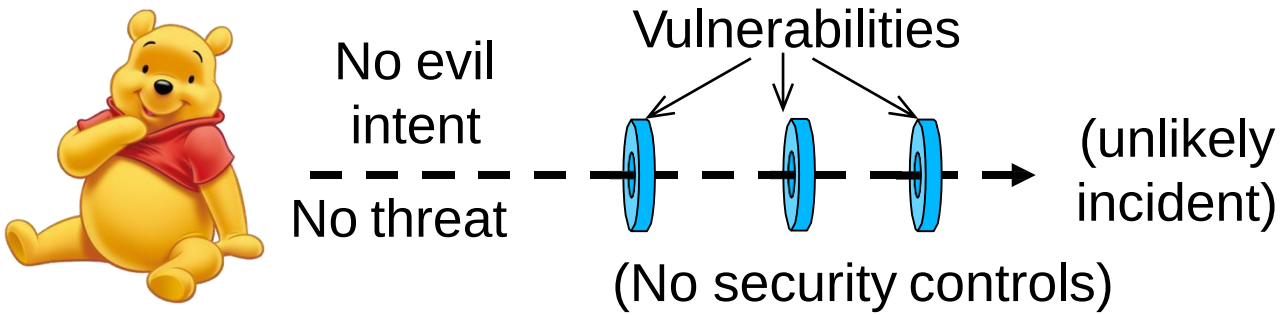
- Multiple different threats (scenarios) can be identified
- Each threat can potentially cause a (different) incident
- Each potential incident has a risk level
- Multiple threats ⇒ Many risks



Likelihood of a security incident







The level of a specific risk

- Practical risk analysis typically considers two factors to determine the level of each risk
  1. Likelihood / frequency of each type of incident
  2. Impact on assets (loss) resulting from each type of incident