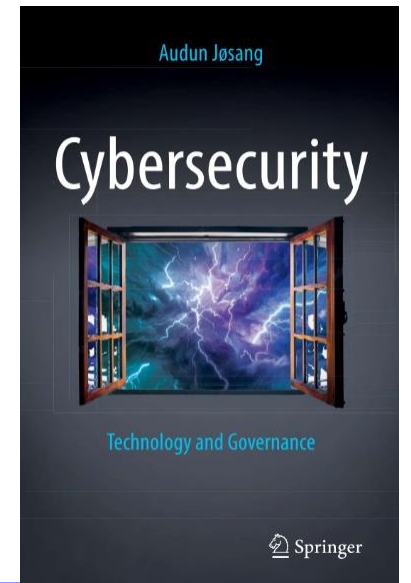


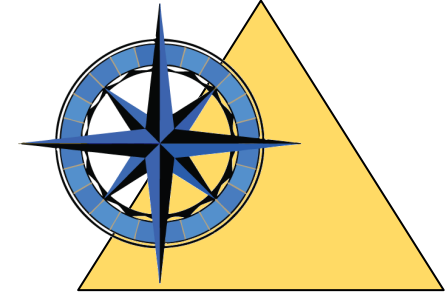
Chapter 19: Cyber Risk Management

Cybersecurity: Technology and Governance

Audun Jøsang,
1st Edition, Springer Nature, 2024.

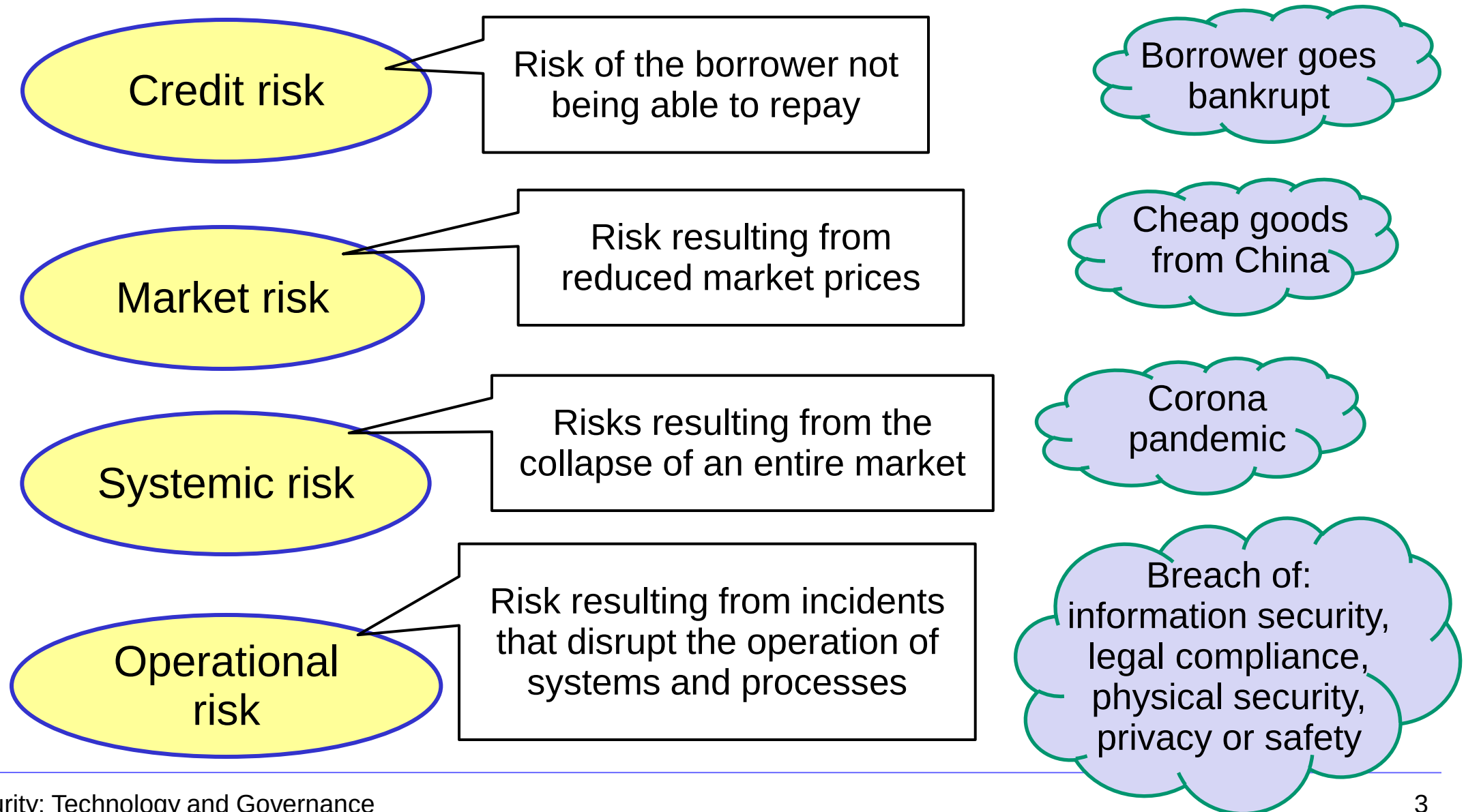


Overview: Risk management



- a. What is risk?
- b. Risk management
- c. Risk assessment
- d. Risk treatment

Types of Risks



What is risk, and information security risk?

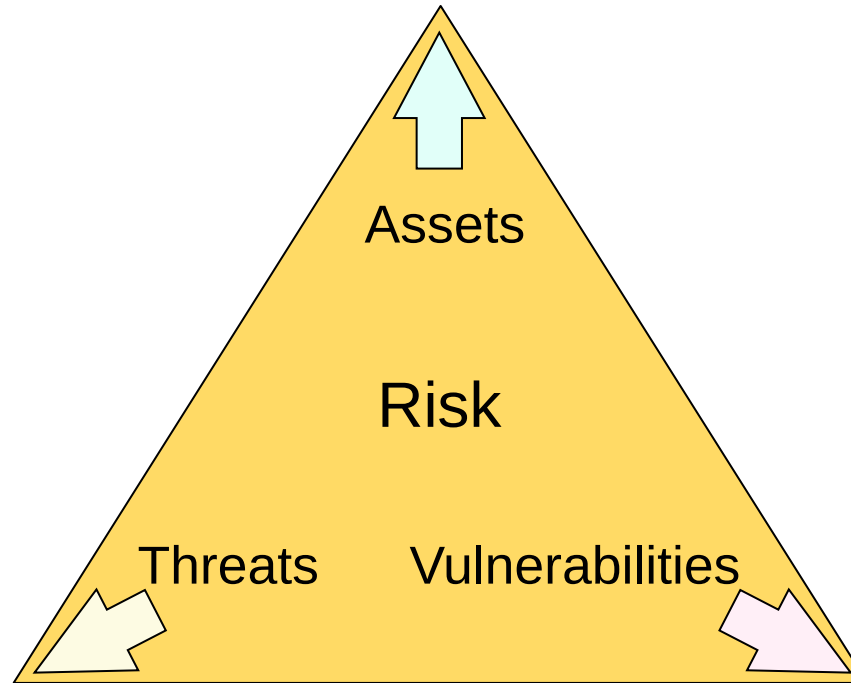
- ISO 31000 Risk management and ISO/IEC 27000 Overview
 - **“Risk is the effect of uncertainty on objectives”**
 - No distinction between positive and negative effects of uncertainty
 - Very general and abstract definition, unsuitable for IS risk assessment
 - But ISO 31000 also states: **Risk is usually expressed in terms of risk sources, potential events, their consequences and their likelihood.**
- ISO/IEC 27005 Guidance on managing information security risks
 - Repeats the definition from ISO 31000, but also provides a specific definition related to information security:
 - **“Information security risks can be associated with the potential that threats will exploit vulnerabilities of an information asset or group of information assets and thereby cause harm to an organization.”**



International
Organization for
Standardization



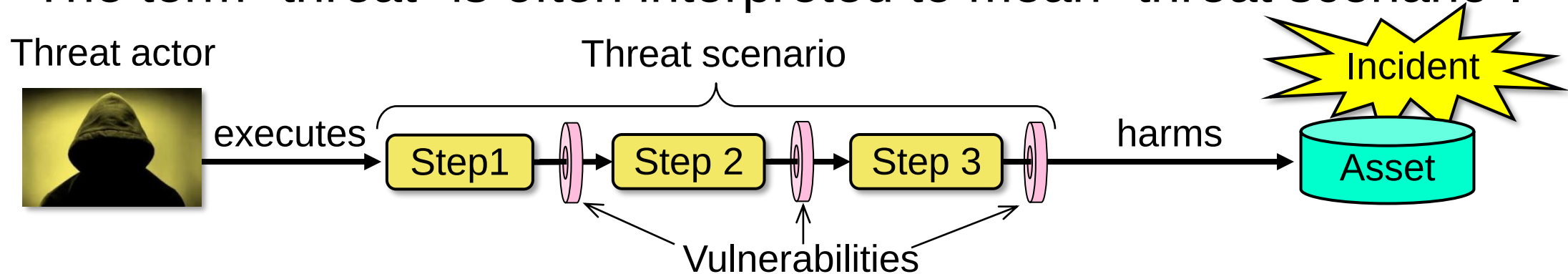
General Risk Model



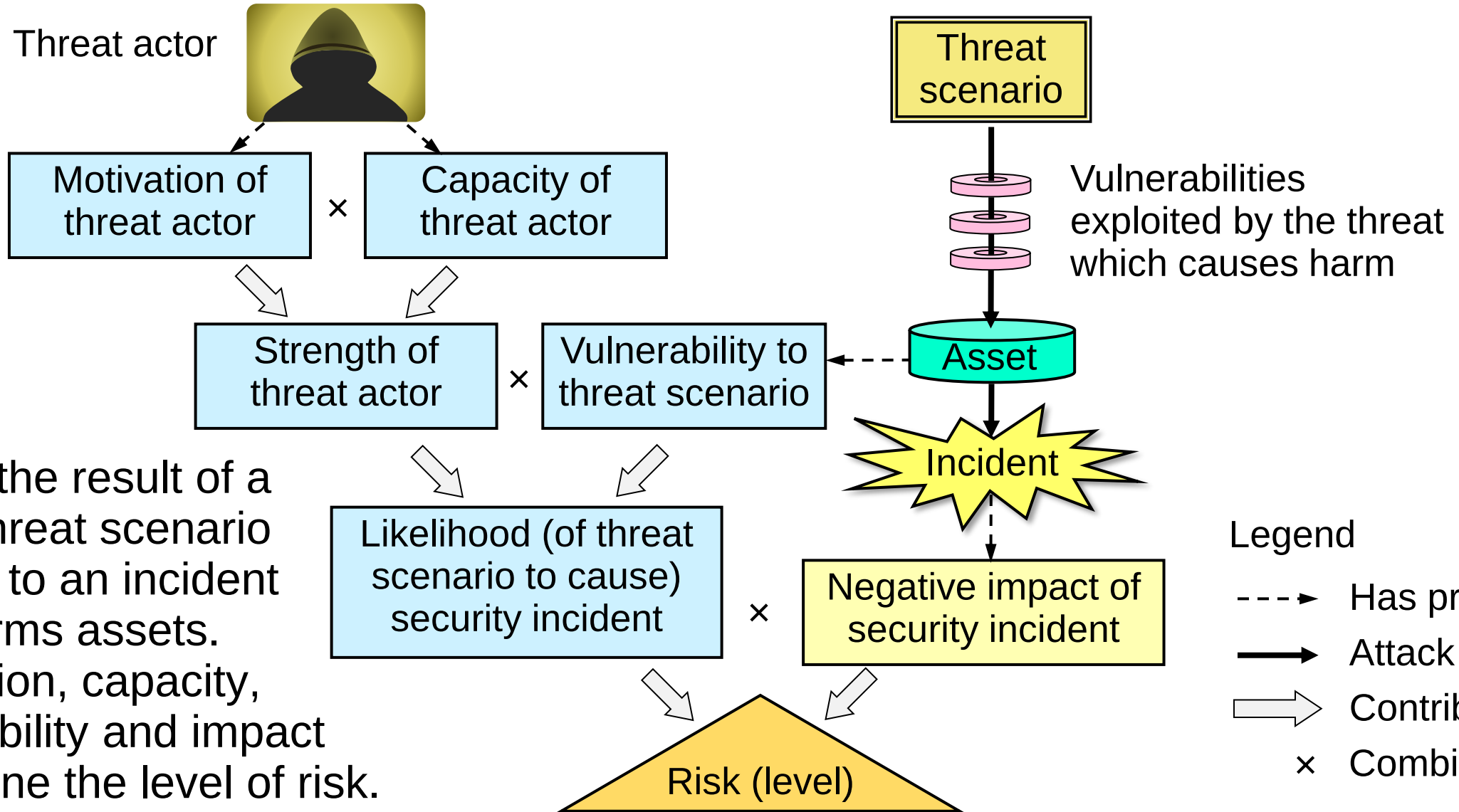
- General risk model
 - The greater the assets, the greater the threats, and the more serious the vulnerabilities, then the greater the risk you are exposed to.

Threats

- **Threat scenario:** A sequence of steps or events that can be controlled or triggered by a threat actor and that can damage assets/resources. A threat scenario is possible to implement when there are vulnerabilities (weaknesses) that can be exploited.
- **Threat actor:** An active entity that can control or trigger threat scenarios. Threat actors can be intelligent adversarial entities, or forces of nature that are too strong or unpredictable for effective prevention.
- The term "threat" is often interpreted to mean "threat scenario".



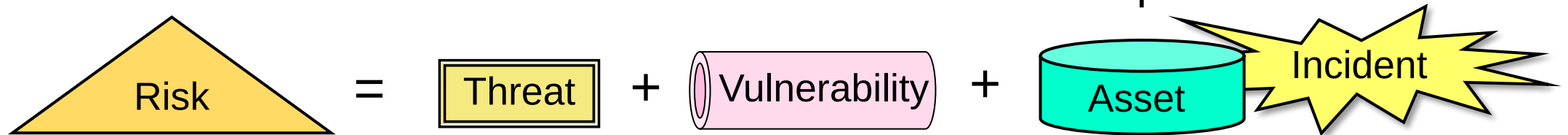
Detailed risk model



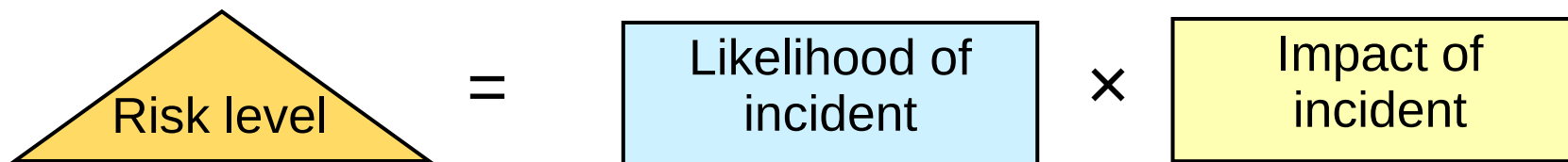
- Risk is the result of a given threat scenario leading to an incident that harms assets.
- Motivation, capacity, vulnerability and impact determine the level of risk.

Risk or risk level?

- In everyday speech, "risk" and "risk level" have similar meanings
 - *What is the risk (risk level) of being hacked with a Trojan?*
- In technical language, there is a clear difference:
 - **Risk** is a relevant combination of threat/vulnerability/potential incident with a breach of CIA for an asset. Risk identification is to map relevant combinations.

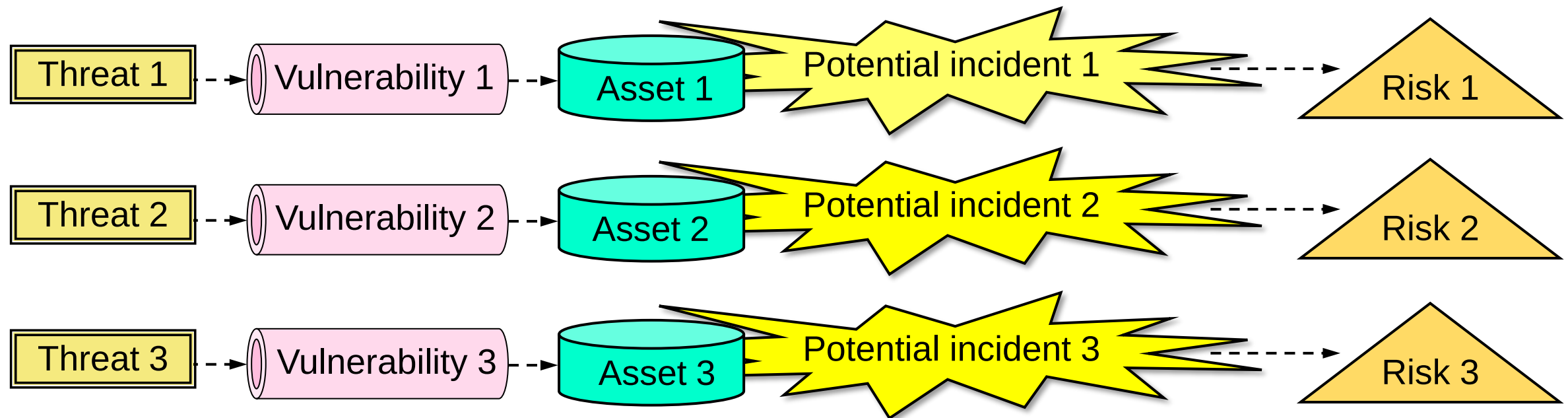


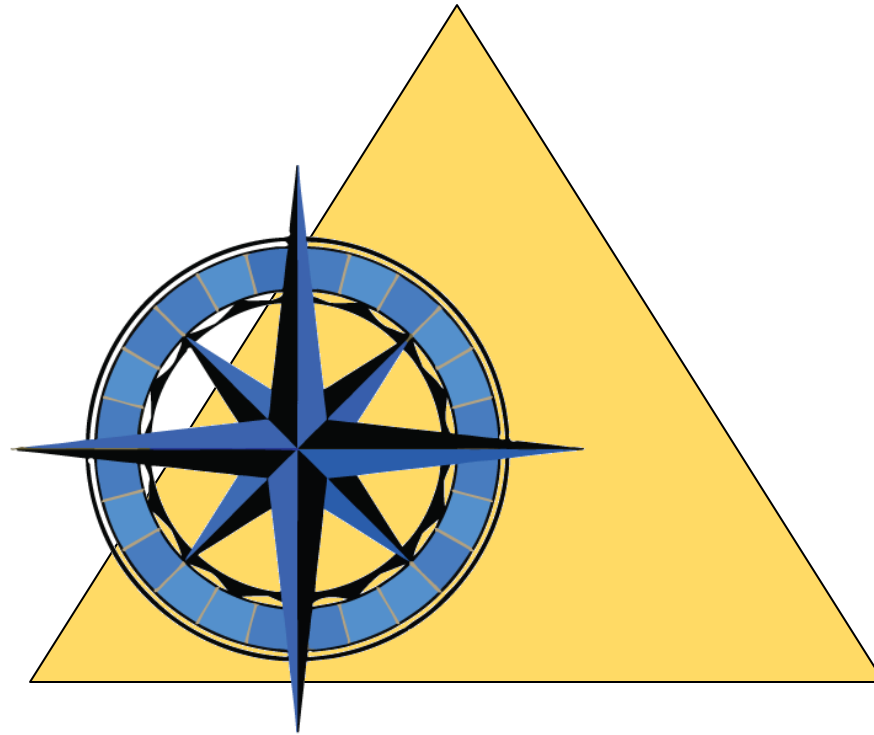
- **Risk level** (also called risk exposure) is the combination of the likelihood and impact of the potential incident. Risk analysis is to compute the risk level.



Many risks

- Several different threats (scenarios) can be identified
- Each threat can exploit vulnerabilities and cause an incident
- Each potential incident can harm an asset to cause negative impact
- Many threats $\Rightarrow$ many risks





Part b: Risk management

Risk Management Standards

- ISO 31000 Risk management



- ISO/IEC 27005 Guidance on managing information security risks



- NIST SP800-39 Managing Information Security Risk
- NIST SP800-30 Guide for Conducting Risk Assessment



What is risk management?

- «Risk management is the coordinated activities to direct and control an organization with regard to risk. » (ISO 31000)
- Risk management activities can have different objectives. For example, it could be one or more of the following:
 - to get an overview of assets
 - To get an overview of threats
 - to get an overview of vulnerabilities
 - to get an overview of existing risks
 - to propose new security controls
 - to assess residual risk following new proposed security controls
 - providing a basis for buying cyber insurance
 - to provide a basis for proposing a budget for risk management



Focus, context, criteria for risk acceptance

- Risk management shall balance identified risks, with investment in security controls.
- Risk management includes conducting a series of risk assessments, each based on a threat scenario:
 - that can cause a security incident that results in a breach of information security for assets, and thus creates negative impacts for the business.
- Methods for risk analysis must be determined
 - E.g. qualitative, relative, quantitative
- Risk acceptance criteria should be defined before starting the risk assessments.



Starting point for assessing IS risk

- Overview of assets: identify and understand the value of information assets and systems.
- Overview of the threats: identify relevant threat scenarios that could harm information and related assets.
- Overview of the vulnerabilities that can be exploited by threats, and thus can lead to incidents.
- Understanding the potential impacts of incidents.
- Clarity on ownership of assets and responsibility for treating the identified risks.

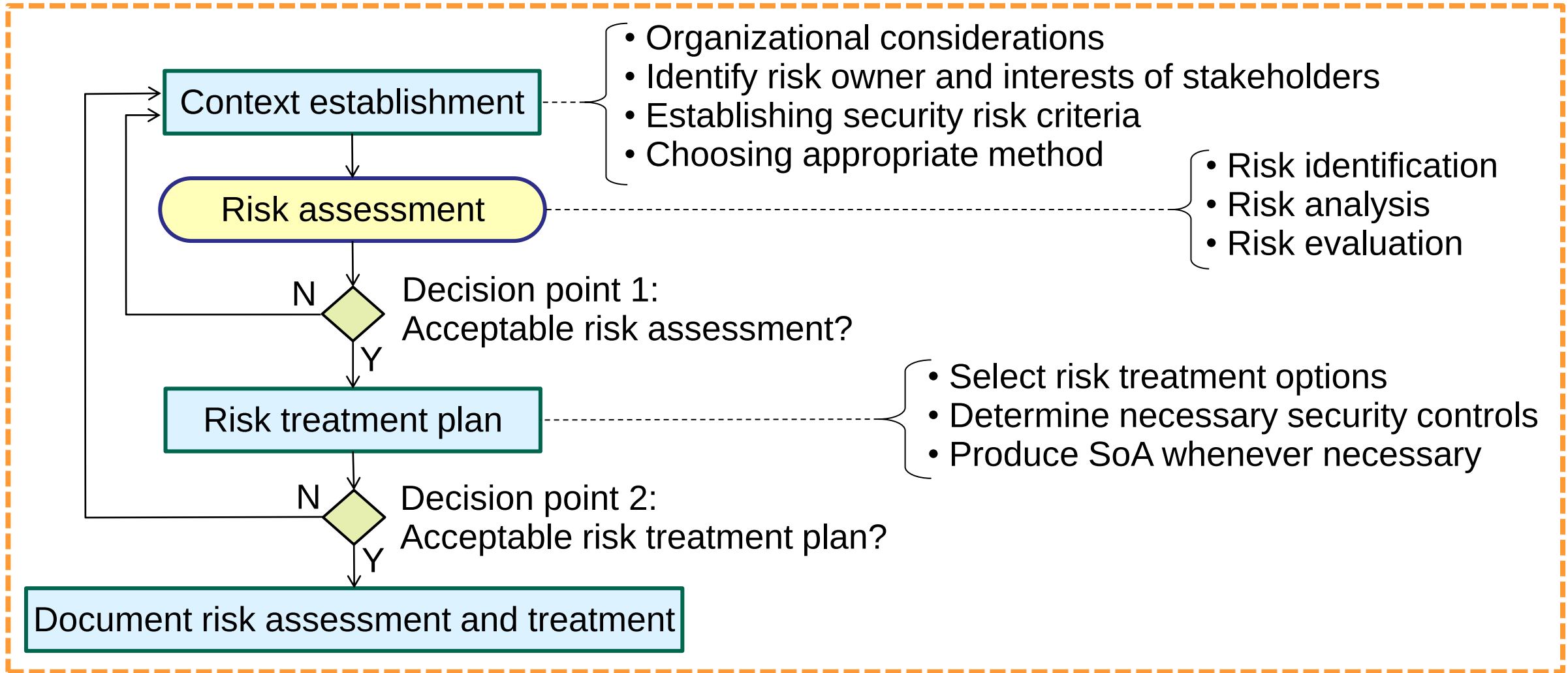
Roles involved in risk assessment



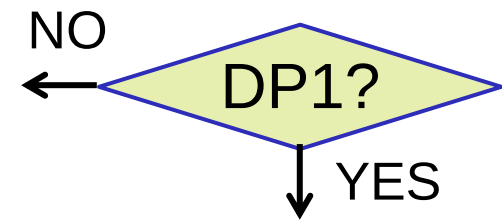
Managers, asset owners, subject matter experts and users must work together.

- Asset owners must help to
 - create an overview of assets, and specify security objectives (CIA)
 - assess impacts of potential breaches of security objectives
- Users and security experts need to help
 - identify threats and vulnerabilities;
 - assess likelihoods
- Risk experts must guide the risk analysis process
- Security experts must advise on security measures
- Management must review the risk management process and approve budget for proposed security controls

Risk management process: ISO/IEC 27005



Decision Point 1

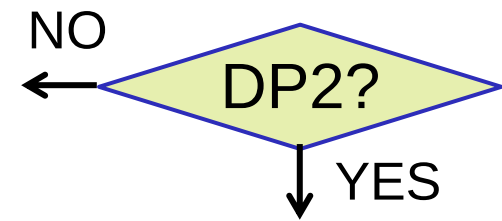


Is the risk assessment satisfactory?

Possible reasons for answering "NO" and how it can be corrected:

- a. Relatively poor distribution of risk levels.
 - The distribution can be improved with recalibration of likelihood and impact levels.
- b. Too much uncertainty about one or more (high) risks.
 - Uncertainty can be reduced by making a more thorough assessment of these risks.

Decision Point 2



Is the risk treatment plan acceptable?

Possible reasons for answering "NO" and how it can be corrected:

a. Too high residual risk

- High residual risk can be lowered by implementing several measures.
- High residual risk can be defined as appropriate by raising the risk threshold.

b. Too low residual risk

- Low residual risk can be raised by implementing fewer measures.
- Low residual risk can be defined as appropriate by lowering the risk threshold.

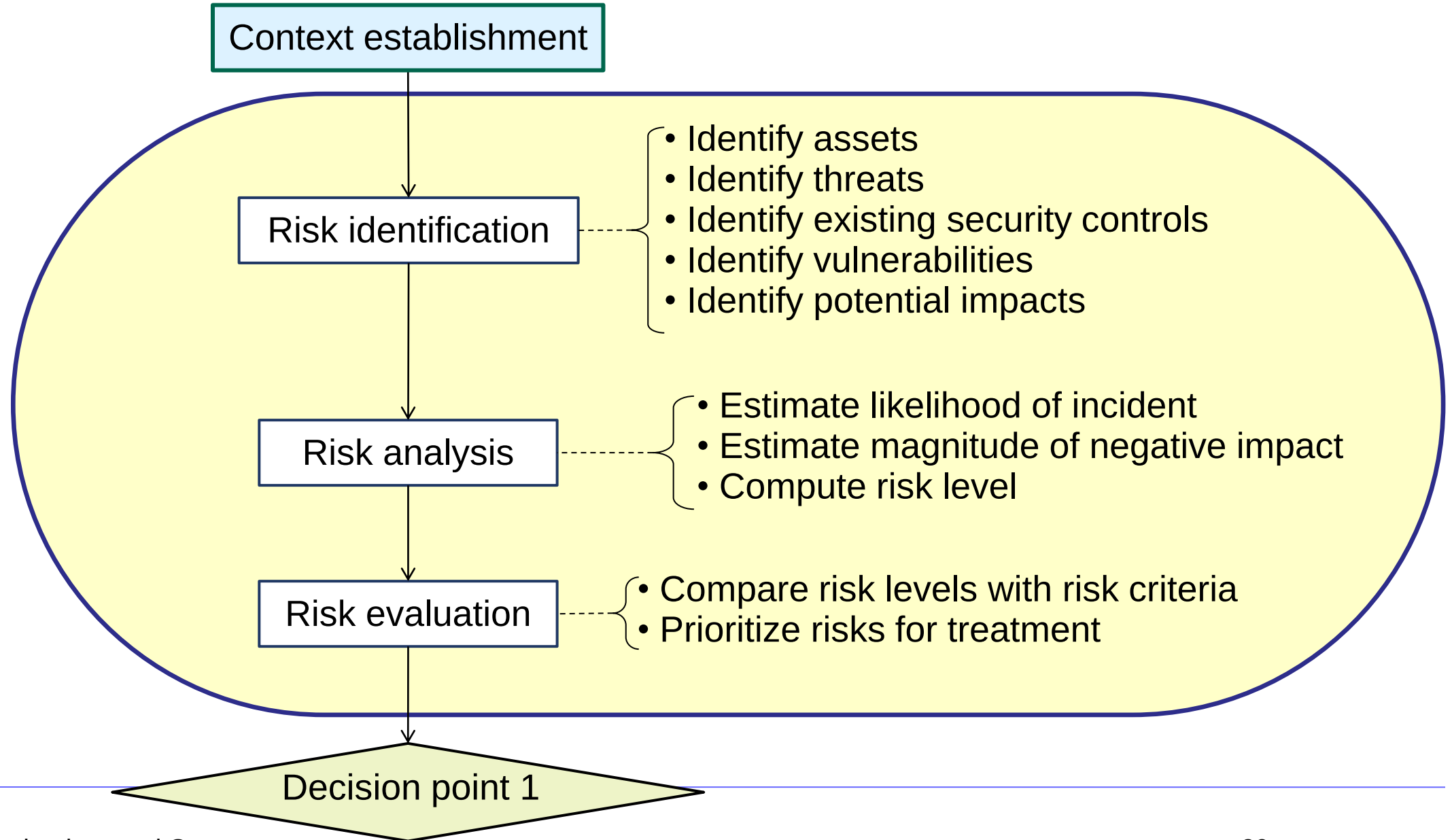
c. Appropriate residual risk, but insufficient budget to introduce proposed risk-reducing measures.

- Adjust budget by increasing budget or cutting measures.

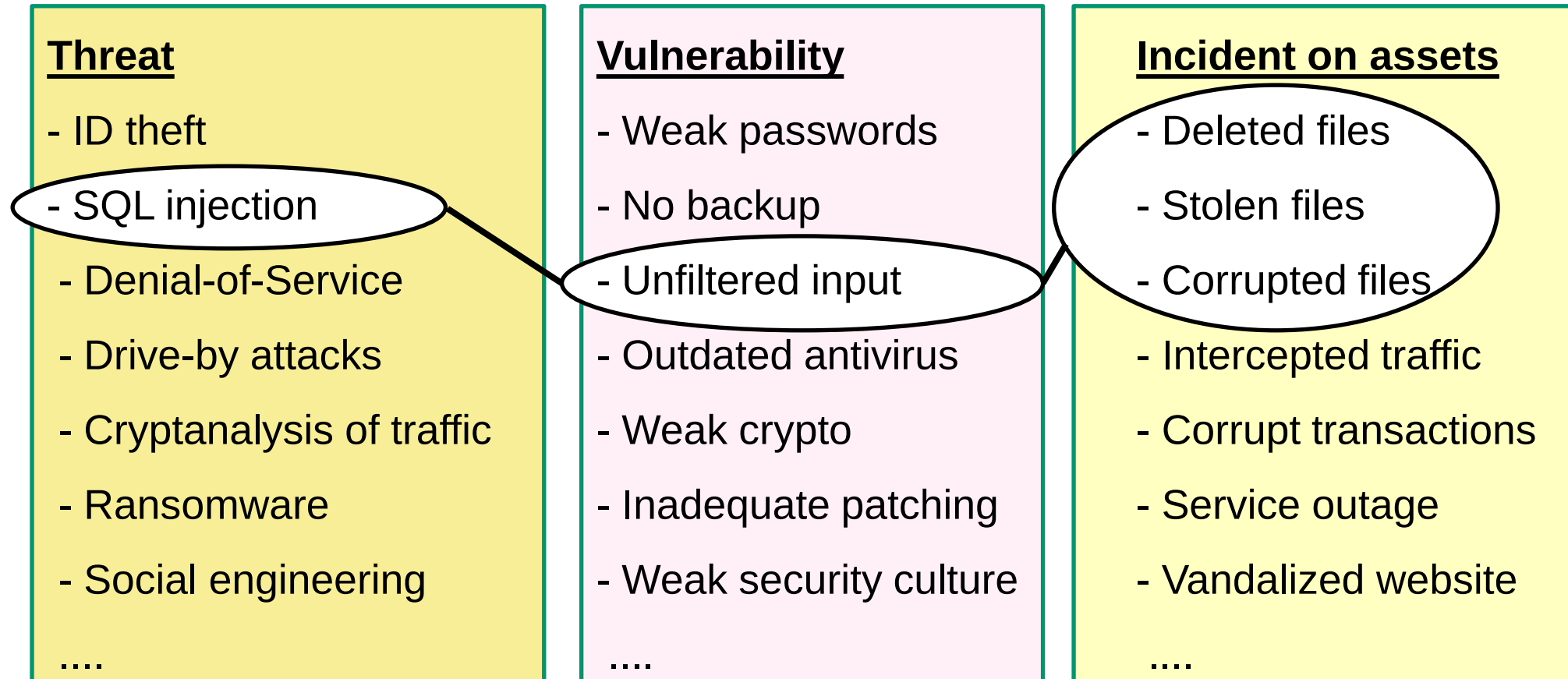
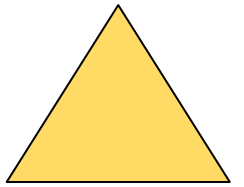


Part c: Risk assessment

Risk assessment process – ISO/IEC 27005



Risk identification



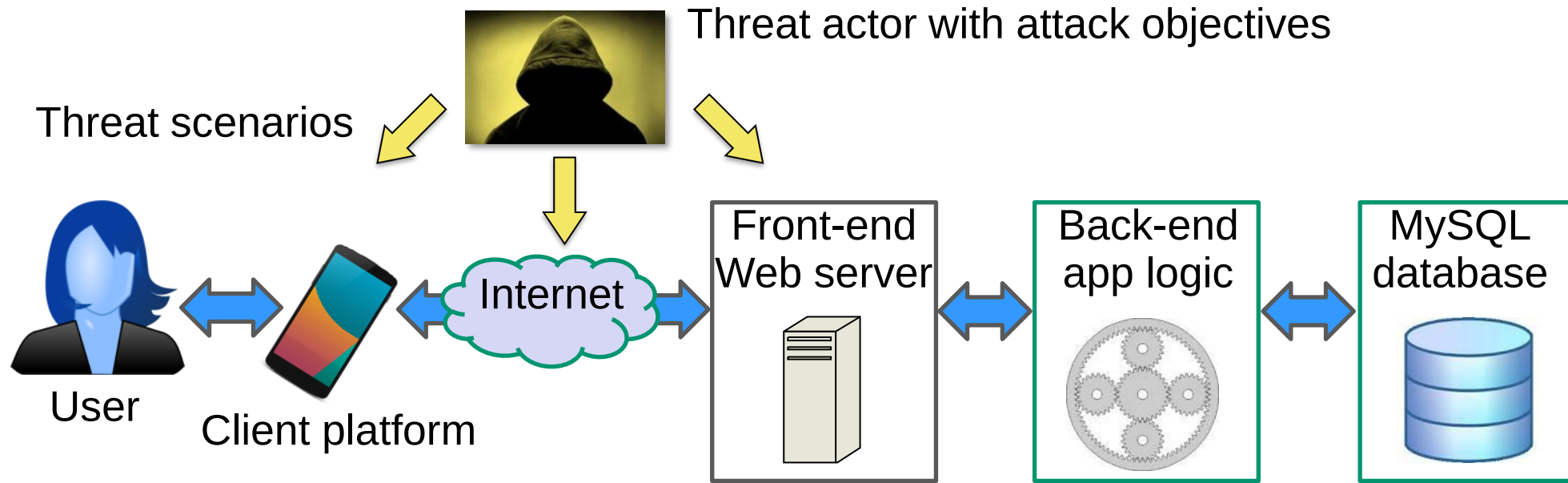
- Identifying a risk means finding a relevant combination of a threat, vulnerability(s) and event(s) that could cause harm to assets.

Identifying Assets



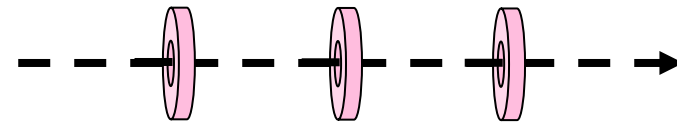
- Wide range of asset types
 - Business data, personal data, systems, networks, applications, people, etc.
 - Consider the CDM (Cyber Defense Matrix) asset types
- Impossible to get a complete overview
 - It is also not important to have a total overview
 - The goal is to point out the most relevant and valuable assets
- Responsibility for identifying assets lies with the owners
 - For that reason asset owners must participate in risk assessment
- For each asset, specify
 - Importance of security objectives (CIA)
 - Possible impacts for breach of security objectives

Threat Modelling



- Threat modelling consists of identifying, analyzing and describing relevant attack scenarios.
- The challenge is to identify relevant threats
- Think: What can happen? How can our values be harmed? Who would be interested in harming us?

Vulnerabilities



- Vulnerabilities are opportunities that threat actors can exploit to attack systems and information assets.
- General identification of vulnerabilities
 - Identifying a security vulnerability is the same as figuring out how to stop a particular threat scenario.
 - Removing a security vulnerability is blocking a threat.
 - A vulnerability is the absence of, or weakness in, controls against a threat.
 - Stopping threats (i.e., removing vulnerabilities) is done with security controls.
- Identification of vulnerabilities with tools and checklists
 - Vulnerability scanners are automated tools for detecting known vulnerabilities in software, systems and networks
 - Vulnerability checklists are used during risk assessment and as part of vulnerability removal efforts, for example with OWASP Top 10.

No vulnerability without a threat

New threat emerged in
Nice in 2016

Promenade des Anglais
Nice, 2020

Promenade des Anglais
Nice, 1980

Nice 2016
Berlin 2016
Barcelona 2017
London 2017, 2018
Magdeburg 2024
New Orleans 2025
Munich 2025

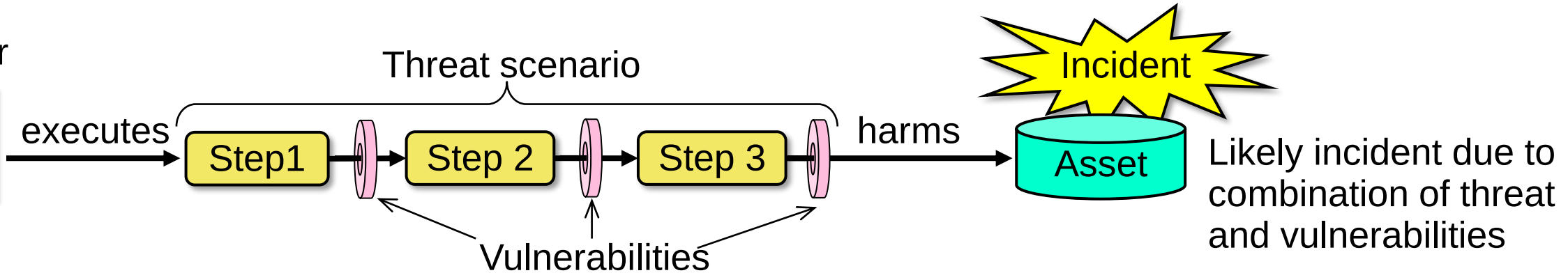


Threat blocked
(i.e., vulnerability removed)

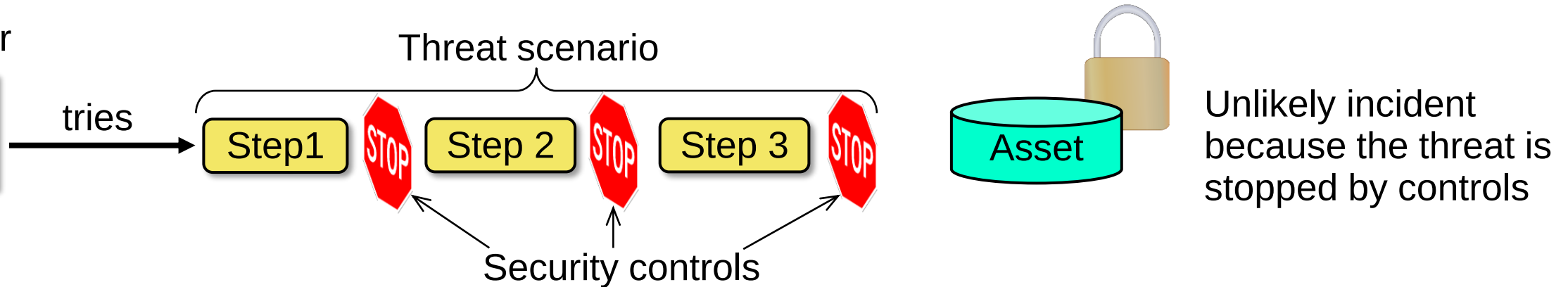


Likelihood of an incident

Threat actor

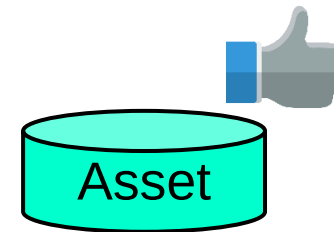
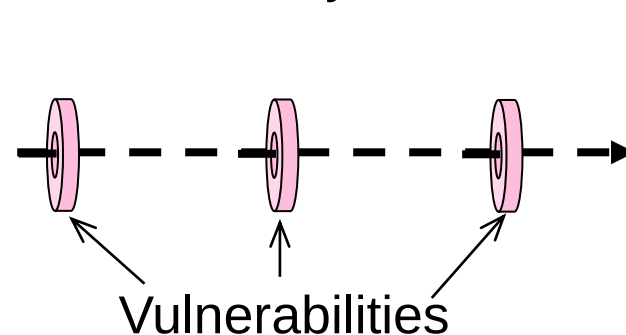


Threat actor



No adversarial intent

No threat actor



Unlikely incident because no threat actor has any adversarial intent

Impact estimation

- An incident leads to a breach of security goals for assets
 - Breach of CIA security goals for assets
 - (Confidentiality, Integrity, Availability)
- The level of impact is estimated for each type of event
- Consequences can consist of different aspects:

- Reduced turnover/profit, loss



- Impaired performance of service



- Violation of legal compliance, legal fees, damages, fines

§

- Damaged reputation



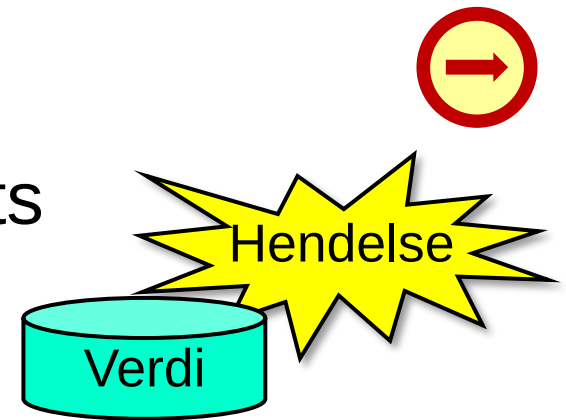
- Costs of handling and recovery



- Strain on employees and users



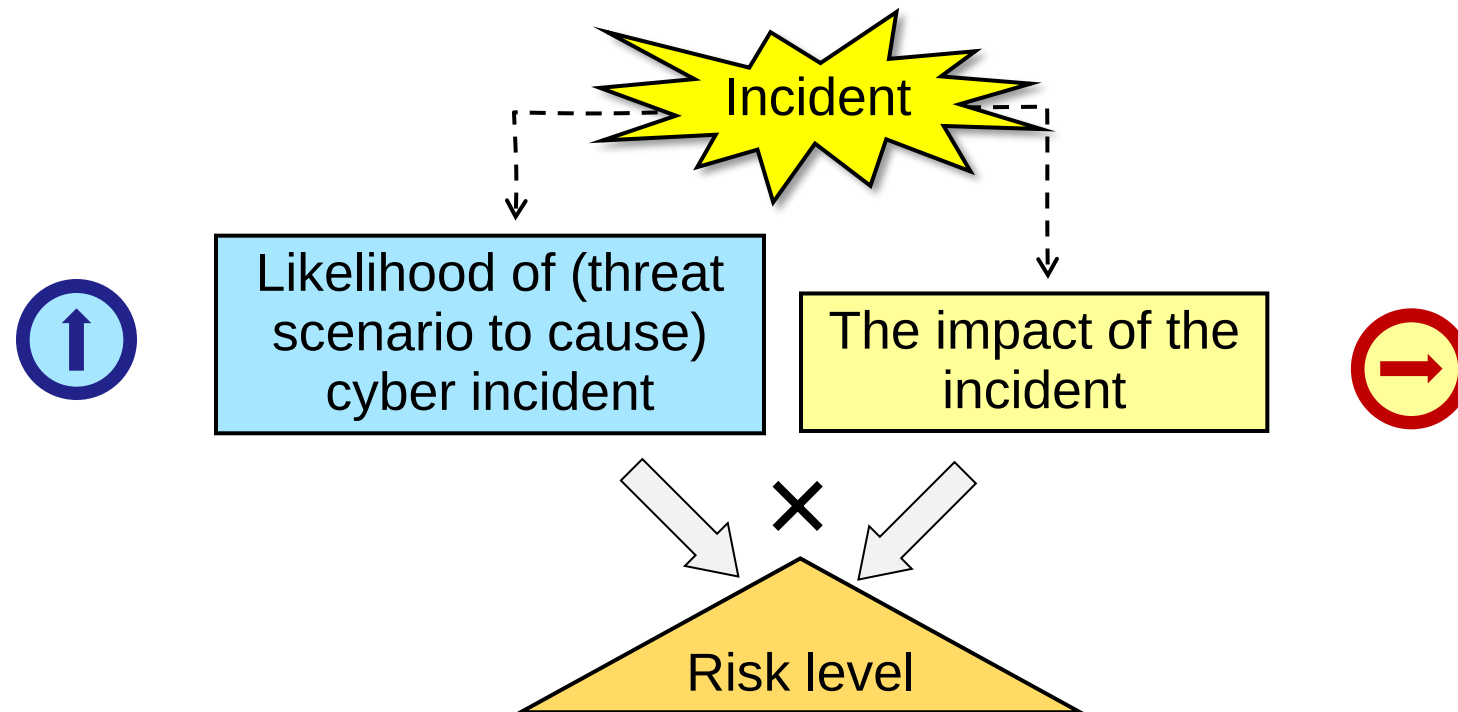
The impact aspects are estimated as a whole.
The highest (most serious) impact is approximately equal to the overall impact.



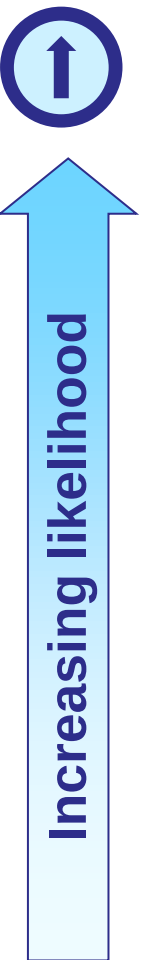
Risk analysis

Practical risk analysis usually considers two factors to determine the level of each risk

- Likelihood (frequency/probability) of each type of incident
- Impact resulting from each type of incident



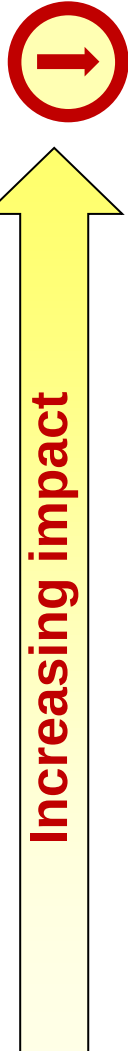
Qualitative likelihood scale



Likelihood	Interpretation
(5) Certain	There are motivated threat actors who can easily achieve attack objectives by implementing the assessed threat scenario for this risk. An incident may already have happened, or will occur shortly, probably within a week.
(4) Likely	Motivated threat actors are likely to achieve attack objectives by executing the identified threat scenario. An incident could occur within a couple of months.
(3) Possible	It may be possible for threat actors to achieve attack objectives using the identified threat scenario. An incident of this type may occur every two years.
(2) Unlikely	Threat actors have little opportunity to achieve attack objectives using the identified threat scenario. It may take decades before an incident occurs.
(1) Rare	Threat actors have no practical opportunity to achieve attack objectives using the identified threat scenario. An incident of this type will probably never occur.

- The scale above is an example. The number of levels and their interpretation can be defined as needed.

Qualitative Impact Scale



Impact	Interpretation
(5) Disastrous	Disastrous harm to assets, services paralyzed, disastrous financial loss and possible bankruptcy. Recovery requires long-term work with large resources. External functions that depend on the business may lapse for a long period.
(4) Major	Major harm to assets, serious service interruption and major financial loss. Considerable resources required to handle the incident. Functions outside the affected business may be adversely affected, but without long-term impacts.
(3) Significant	Significant harm to assets that can result in significant service interruption and significant financial loss. Recovery and service continuity require significant work. Probably little impact on functions outside the affected business.
(2) Minor	Minor harm to assets or operations, and probably little or no service interruption. Just small financial loss. Can be handled with moderate resources.
(1) Insignificant	Insignificant harm to assets, and without any service interruption. The incident is easily handled as part of routine operations. Little or no financial loss.

- The scale above is an example. Levels and interpretation can be defined as needed.

Heat map for qualitative risk analysis

The heat map is a lookup table with predefined risk levels in each cell

Risk level interpretations:

(9 – 10)

E:

Extreme risk; must be treated with priority

(7 – 8)

H:

High risk; should normally be treated

(5 – 6)

M:

Moderate risk; treatment should be considered

(3 – 4)

L:

Low risk; can normally be accepted

(1 – 2)

N:

Negligible risk; can be ignored



Qualitative
likelihood

(5) Certain	(5) M	(7) H	(8) H	(9) E	(10) E
(4) Likely	(4) L	(5) M	(7) H	(8) H	(9) E
(3) Possible	(3) L	(4) L	(5) M	(7) H	(8) H
(2) Unlikely	(2) N	(3) L	(4) L	(6) M	(6) M
(1) Rare	(1) N	(2) N	(3) L	(4) L	(4) L
Qualitative risk levels	(1) Insignificant	(2) Minor	(3) Significant	(4) Major	(5) Disastrous

Qualitative impact levels



Exponentiation and logarithm



- Exponentiation is to “raise base B to the power of X ”
 - means to multiply B by itself X number of times
 - E.g. base $B=10$ raised to the power X is written 10^X
 - Let $B=10$ and $X=3$, then we have $10^3 = 10 \cdot 10 \cdot 10 = 1000$
- Logarithm is to find the exponent to which the base is raised: $\log(B^X) = X$
- E.g. with base $B=10$ we have:
 - $\log(1000) = 3$, because $1000 = 10^3$
 - $\log(0.001) = -3$, because $0.001 = 10^{-3} = \frac{1}{1000}$
- Exponentiation and logarithm are inverse functions
- Logarithmic scale has steps formed by a sequence of exponents,
 - Steps 0.001; 0.01; 0.1; 1; 10; 100; 1000 has logarithmic scale by -3, -2, -1, 0, 1, 2, 3

Relative risk analysis

- Likelihood and impact are represented as relative values in the range [0, 1]
- Relative likelihood 1.0 is interpreted as the highest frequency of occurrence
 - i.e. likelihood 1.0 = N times per year, which e.g. can be 365 (every day) or 50 (every week).
- Relative impact 1.0 is interpreted as the greatest possible loss
 - i.e. impact 1.0 = <extreme loss>, which e.g. can be the market value of the company or less.
- Relative value expressed as 10^X
- Exponent $X = \text{Ordinal level} - 5$
- Produces logarithmic scale
- Relative risk is $R_{\text{Rel}} = P_{\text{Rel}} \cdot V_{\text{Rel}}$
-

Qualitative ordinal levels of likelihood (P_{Qual}) and impact (V_{Qual})		Relative levels of likelihood (P_{Rel}) and impact (V_{Rel})
Ordinal level 5	($X = 5 - 5 = 0$)	$10^X = 10^0 = 1.0000$
Ordinal level 4	($X = 4 - 5 = -1$)	$10^X = 10^{-1} = 0.1000$
Ordinal level 3	($X = 3 - 5 = -2$)	$10^X = 10^{-2} = 0.0100$
Ordinal level 2	($X = 2 - 5 = -3$)	$10^X = 10^{-3} = 0.0010$
Ordinal level 1	($X = 1 - 5 = -4$)	$10^X = 10^{-4} = 0.0001$

Conversion between relative and qualitative risk

- Relative risk: $R_{\text{Rel}} = 10^Z$, where $Z = X + Y = P_{\text{Qual}} - 5 + V_{\text{Qual}} - 5 = R_{\text{Qual}} - 10$
- Principle for logarithm: $\log(10^X) + \log(10^Y) = X + Y = \log(10^{(X+Y)}) = \log(10^X \cdot 10^Y)$
 - Qualitative likelihood: $P_{\text{Qual}} = \log(P_{\text{Rel}}) + 5 = \log(10^X) + 5$, where $X = P_{\text{Qual}} - 5$
 - Qualitative impact: $V_{\text{Qual}} = \log(V_{\text{Rel}}) + 5 = \log(10^Y) + 5$, where $Y = V_{\text{Qual}} - 5$
 - Qualitative risk: $R_{\text{Qual}} = \log(R_{\text{Rel}}) + 10$
 - $= \log(P_{\text{Rel}} \cdot V_{\text{Rel}}) + 10$
 - $= \log(P_{\text{Rel}}) + \log(V_{\text{Rel}}) + 10$
 - $= \log(10^X) + \log(10^Y) + 10$
 - $= P_{\text{Qual}} - 5 + V_{\text{Qual}} - 5 + 10$
 - $= P_{\text{Qual}} + V_{\text{Qual}}$

Quantitative likelihood estimates

- The quantitative likelihood scale is logarithmic
- N is the likelihood calibration factor for highest expected occurrence frequency
- Lesser likelihoods are then determined logarithmically
- Let $N = 50$ (i.e. 50 times per year, which is approximately once per week).
- Quantitative likelihood: $P_{\text{Quan}} = N \cdot P_{\text{Rel}}$
- Exponent $X = \text{ordinal qualitative likelihood} - 5$

Qualitative ordinal levels of likelihood (P_{Qual})	Quantitative levels of likelihood (P_{Quan})	Interpretation
Ordinal level 5 ($X = 5 - 5 = 0$)	$P_{\text{Quan}} = N \cdot 10^X = 50 \cdot 10^0 = 50.000$	50 times per year = Every week
Ordinal level 4 ($X = 4 - 5 = -1$)	$P_{\text{Quan}} = N \cdot 10^X = 50 \cdot 10^{-1} = 5.000$	5 times per year = Every two months
Ordinal level 3 ($X = 3 - 5 = -2$)	$P_{\text{Quan}} = N \cdot 10^X = 50 \cdot 10^{-2} = 0.500$	Every two years
Ordinal level 2 ($X = 2 - 5 = -3$)	$P_{\text{Quan}} = N \cdot 10^X = 50 \cdot 10^{-3} = 0.050$	Once per 20 years
Ordinal level 1 ($X = 1 - 5 = -4$)	$P_{\text{Quan}} = N \cdot 10^X = 50 \cdot 10^{-4} = 0.005$	Once per 200 years

Quantitative impact estimates



- The quantitative impact scale is logarithmic
- M is the impact calibration factor for highest expected loss
- Lesser impacts are then determined logarithmically
- Let $M = \$10 \text{ million} = \$10^7$
- Quantitative impact: $V_{\text{quan}} = M \cdot V_{\text{Rel}}$
- Exponent $Y = \text{ordinal qualitative impact} - 5$

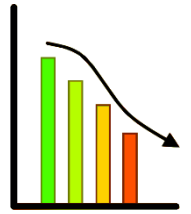
Qualitative ordinal levels of impact (V_{Qual})	Quantitative levels of impact (V_{Quan})	Interpretation
Ordinal level 5 ($Y = 5 - 5 = 0$)	$M \cdot 10^Y = 10^7 \cdot 10^0 = 10^7$	$V_{\text{Quan}} = \$10 \text{ million}$
Ordinal level 4 ($Y = 4 - 5 = -1$)	$M \cdot 10^Y = 10^7 \cdot 10^{-1} = 10^6$	$V_{\text{Quan}} = \$1 \text{ million}$
Ordinal level 3 ($Y = 3 - 5 = -2$)	$M \cdot 10^Y = 10^7 \cdot 10^{-2} = 10^5$	$V_{\text{Quan}} = \$100 \text{ 000}$
Ordinal level 2 ($Y = 2 - 5 = -3$)	$M \cdot 10^Y = 10^7 \cdot 10^{-3} = 10^4$	$V_{\text{Quan}} = \$10 \text{ 000}$
Ordinal level 1 ($Y = 1 - 5 = -4$)	$M \cdot 10^Y = 10^7 \cdot 10^{-4} = 10^3$	$V_{\text{Quan}} = \$1000$

Quantitative risk computation



- Quantitative risk: $R_{\text{Quan}} = P_{\text{Quan}} \cdot V_{\text{Quan}}$
 $= N \cdot P_{\text{Rel}} \cdot M \cdot V_{\text{Rel}}$
 $= N \cdot M \cdot R_{\text{Rel}}$, where $N = \text{max frequency/year}$, $M = \text{max impact}$
 $= N \cdot M \cdot 10^X \cdot 10^Y$, where $X = P_{\text{Qual}} - 5$ and $Y = V_{\text{Qual}} - 5$
 $= N \cdot M \cdot 10^Z$, where $Z = X + Y = R_{\text{Qual}} - 10$
- Assume that for a given risk the estimated impact V_{Quan} is bankruptcy, and the estimated likelihood P_{Quan} is once per week, then of course it doesn't mean that the company goes bankrupt every week.
- In addition, if a lesser risk does materialize, it typically only happens once, since the company will learn from the incident and will recover to a more secure state.
- For such risks, the expected loss is equal to the estimated impact V_{Quan} , where the estimated likelihood P_{Quan} indicates how soon that loss is predicted to materialise.
- In any case, the product $R_{\text{Quan}} = P_{\text{Quan}} \cdot V_{\text{Quan}}$ indicates the severity of that risk relative to other risks.

Impact assessment with multiple aspects



- A single risk can have multiple different impacts
- For qualitative and relative impact estimation, we typically use the highest among the relevant impacts for the specific risk.
- For quantitative estimation, the impact V_{Quan} can be expressed as an absolute monetary value
 - Overall impact for a given risk is the sum of impact aspect values.
 - Assume four impact aspects v_1, v_2, v_3, v_4

$$\text{Then } V_{\text{Quan}} = v_1 + v_2 + v_3 + v_4$$



Case: Hacking of website

- Risk: Defaced and broken website
- Probability estimate
 - $P_{\text{Quan}} = 0.5$, i.e. it is likely to happen every 2 years
- Impact estimate with multiple aspects
 - Lost profit because the website is down, $v_1 = \$50,000$
 - Lost reputation $v_2 = \$20,000$
 - Cost of correcting the web page $v_3 = \$10,000$
 - $V_{\text{Quan}} = v_1 + v_2 + v_3 = \$80,000$
- Risk computation
 - $R_{\text{Quan}} = P_{\text{Quan}} \cdot V_{\text{Quan}} = 0.5 \times \$80,000 = \$40,000$ expected loss per year
- Can justify spending \$40,000 on security controls to manage risk
 - if the controls will reduce the risk level to \$0

Example qualitative and quantitative risk analysis

Case: Phishing attack for stealing credentials

- Risk: Attacker sends phishing email for tricking victim into revealing credentials
- Likelihood estimation
 - Likelihood calibration factor for highest likelihood frequency $N = 50$ times/year
 - Qualitative likelihood estimate $P_{\text{Qual}} = \textbf{Unlikely}$ (ordinal likelihood level 2)
 - Quantitative likelihood estimate $P_{\text{Quan}} = N \cdot 10^{(2-5)} = N \cdot 10^{-3} = 50 \cdot 0.001 = 0.05$ (once per 20 years)
- Impact estimate
 - Impact calibration factor for highest possible impact $M = \$10 \text{ million} = \$10^7$
 - Qualitative impact estimate $V_{\text{Qual}} = \textbf{Major}$ (ordinal impact level 4)
 - Quantitative impact estimate $V_{\text{Quan}} = M \cdot 10^{(4-5)} = M \cdot 10^{-1} = 10^7 \cdot 0.1 = \$10^6 = \$1 \text{ million}$
- Risk computation
 - $R_{\text{Quan}} = P_{\text{Quan}} \cdot V_{\text{Quan}} = 0.05 \times \$1,000,000 = \$50,000$
- Can justify spending \$50,000 on security controls to manage risk
 - if the controls will reduce the risk level to \$0

Risk assessment spreadsheet

- Many different guides, templates and tools for risk assessment
 - Often relatively complicated, requiring training to use
- Ordinal qualitative estimates of likelihood and impact are logarithmic
- Logarithmic levels make qualitative risk computation additive
 - $R_{\text{Qual}} = P_{\text{Qual}} + V_{\text{Qual}}$
- Quantitative risk computation is multiplicative

$$R_{\text{Quan}} = P_{\text{Quan}} \cdot V_{\text{Quan}}$$

- UiO spreadsheet for qualitative and quantitative cyber risk assessment:

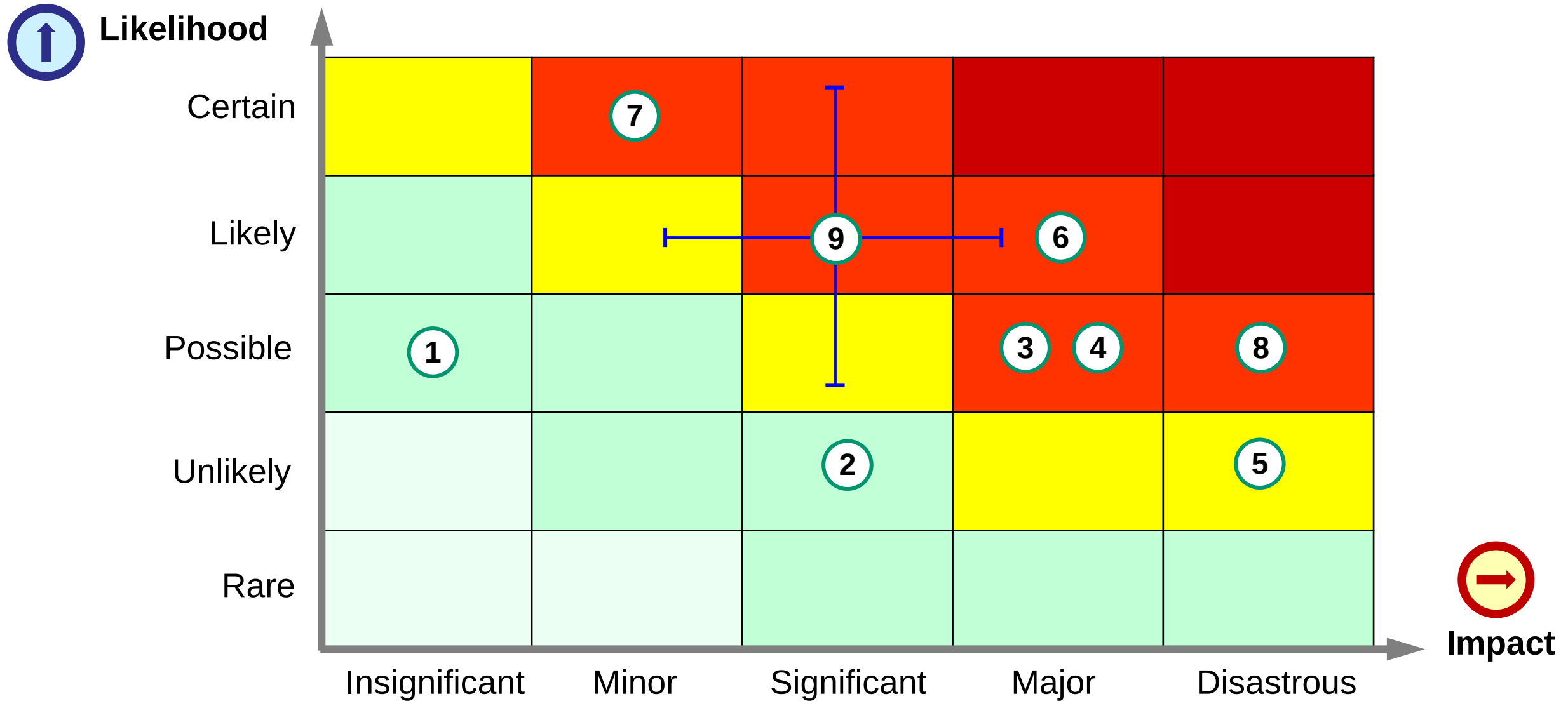
<https://www.mn.uio.no/ifi/english/research/groups/sec/instructional/UiO-risk-assessment.xlsx>

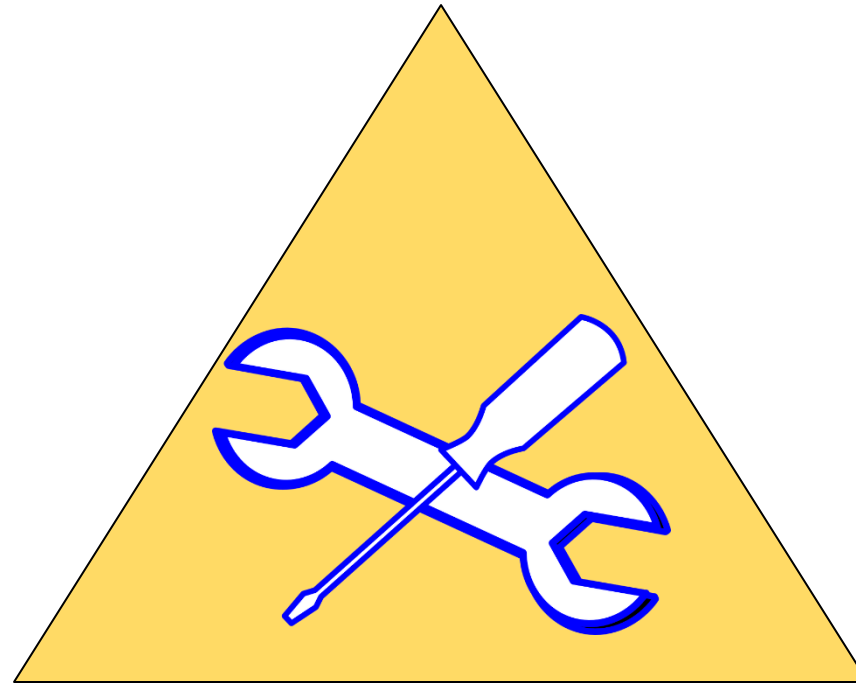
- Threat
 - Threat scenario and possible threat actor
- Vulnerability
 - Which weaknesses and flaws allow the threat scenario to be implemented
- Affected assets
 - Describes incident (breach of security objectives)
- Impacts
 - Describe the expected consequences of the incident
- Existing likelihood-reducing or impact-reducing controls
 - Controls that are already intended to prevent the threat scenario or mitigate the impacts
- Detection and investigation
 - How can such an event (or stage of the threat scenario) be detected and investigated?
- Calculating risk level with spreadsheets
 - a) qualitative risk = qualitative likelihood + qualitative impact
 - a) relative risk = relative likelihood × relative impact
 - b) quantitative risk = quantitative likelihood × quantitative impact
- Recommended new controls
 - Proposals for new security controls to prevent the incident or mitigate the impacts

Use of the spreadsheet

- Assumptions:
 - identification of assets, threats and vulnerabilities is done separately
 - estimation of likelihoods and impact levels is done separately
- Risk calculations are done both before and after new controls
 - The risk level is generally calculated before new controls
 - The risk level can also be calculated with the assumption of new controls
- Cost of new controls is not included in spreadsheet
 - Estimation of the cost of new controls can be described separately
 - Return On Investment (ROI) can be described separately, and will require quantitative estimation/calculation of cost of controls and quantitative risk levels.

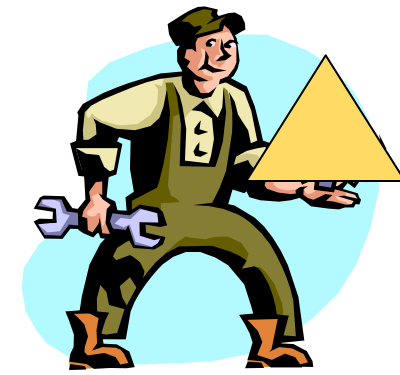
Risk visualisation





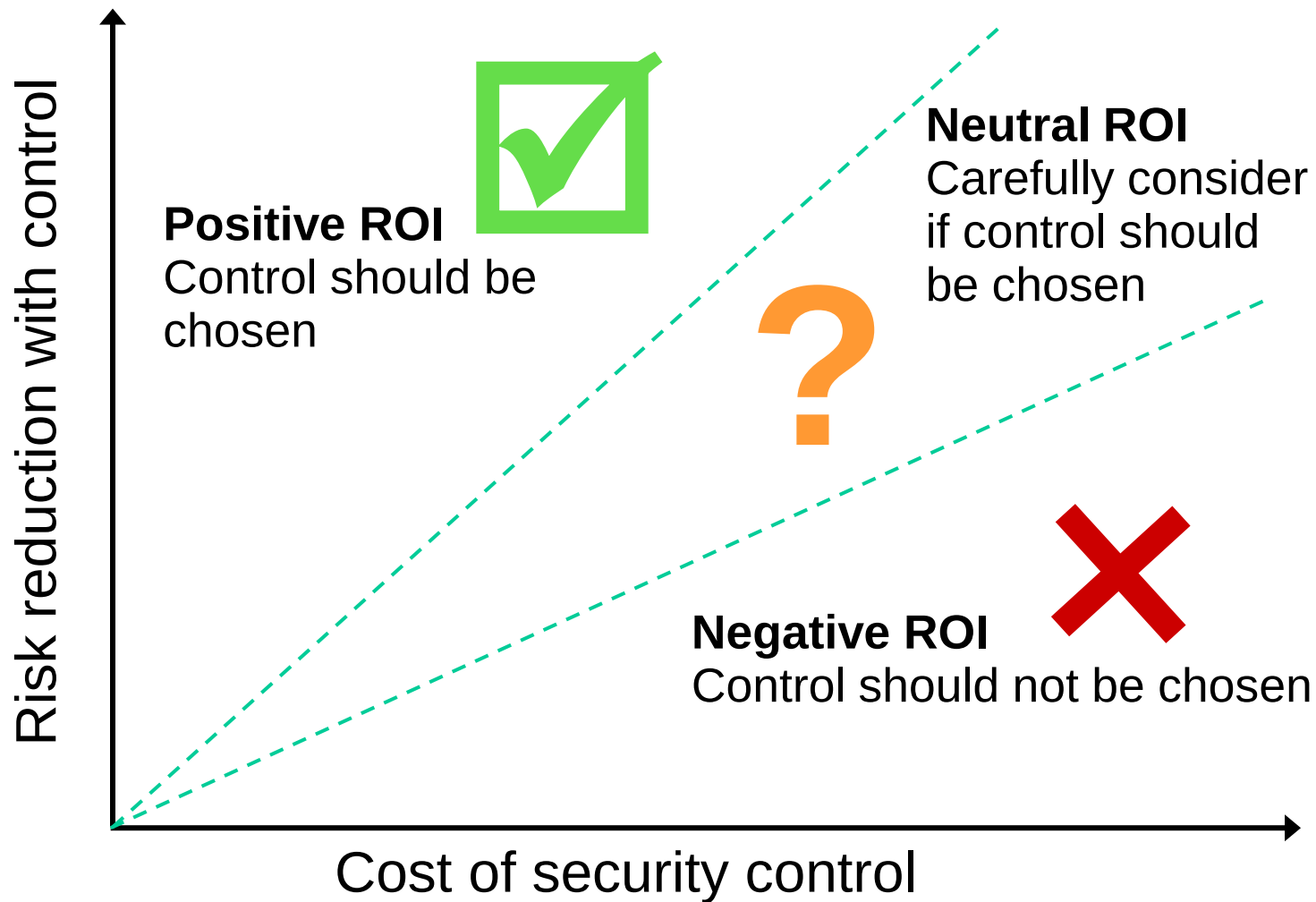
Part d: Risk treatment

Risk treatment



- Sort the identified and assessed risks by level/severity.
- For each unacceptable risk, choose one of four ways to treat it.
 1. Reduce risk by implementing security controls. Can be selected from standards such as ISO/IEC 27002, NIST CSF or CSC.
 2. Share/transfer the risk (outsource activity that causes the risk). Alternatively, purchase cyber insurance.
 3. Retain risk (understand and tolerate potential impacts)
 4. Avoid the risk (stop activity that causes the risk)

ROI for security controls (Return on Investment)



$$ROI = \frac{\text{Profit} - \text{Investment}}{\text{Investment}}$$

$$ROI = \frac{\text{Risk reduction} - \text{Cost}}{\text{Cost}}$$

Sharing/Transferring Risk



- Risk treatment option that intends to share or shift risk to other entities, processes, or organizations
- For example, the organisation may transfer risks associated with the operation of complex systems to another organisation with greater expertise in managing these risks
- Alternatively, the organization can purchase insurance against potential losses caused by security incidents, which is called cyber insurance.

Retaining risk



- Alternative that consists of doing nothing to manage a risk further, which thus means accepting the risk as it is.
- Prudent only when the level of risk is relatively low in relation to the costs of treatment/introduction of controls.
- Risk appetite describes the extent to which the organization is willing to accept risk as a trade-off against the costs of treatment.

Risk avoidance



- Any business activity carries a certain amount of risk, but the benefits and profits normally outweigh the risks.
-
- In the event that the risk is too high compared to the benefits and profits, and it is not possible to reduce, mitigate, transfer or retain the risk, the last resort is to stop the business activity that entails risk.
-
- Be aware of the risk of lost benefit and profit by not conducting a business activity.
- A decision to stop a business activity should be taken at a senior management level.

Risk treatment and residual risk

- For each priority risk, identify potential actions or other management that will mitigate the risk.



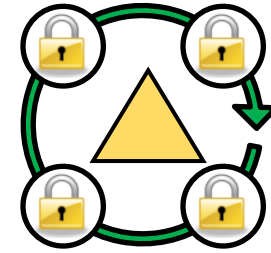
- Residual risk is the risk that remains after handling.
- It is a management decision to accept residual risk. The accepted residual risk must be justifiable in accordance with the company's risk strategy.

Mitigating residual risk



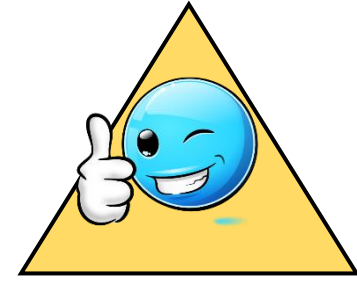
- Attempts to mitigate the negative impact of security incidents through planning and readiness
- Approaches for mitigating residual risk:
 - Incident Response Plan (IRP)
 - Disaster Recovery Plan (DRP)
 - Business Continuity Plan (BCP)

Evaluation and maintenance of risk management controls



- Implementing controls to reduce risk is not the end of the process.
- Treatment and associated controls must be operated and evaluated on an ongoing basis to determine efficiency and assess the residual risk more accurately
- The process continues as long as your organization continues to have business activities that carry risk.
- Risk management is a process, not an end state!

Positive view of risk



- Identify options for risk management by seeking alternative business models that can increase positive benefits and profits without increasing risk accordingly.
- Options include:
 - Actively seek business opportunities, even if it involves risks
 - Increase benefits and profits without increasing risk accordingly
 - Share business opportunities and risks with other players
 - Know the residual risk, and be prepared to handle incidents
 - Know the residual risk, and be prepared to justify it if an incident occurs

End of presentation