SYKEHUSPARTNER

UNIVERSITY OF OSLO

An Opportunity-Based Approach to Information Security Risk

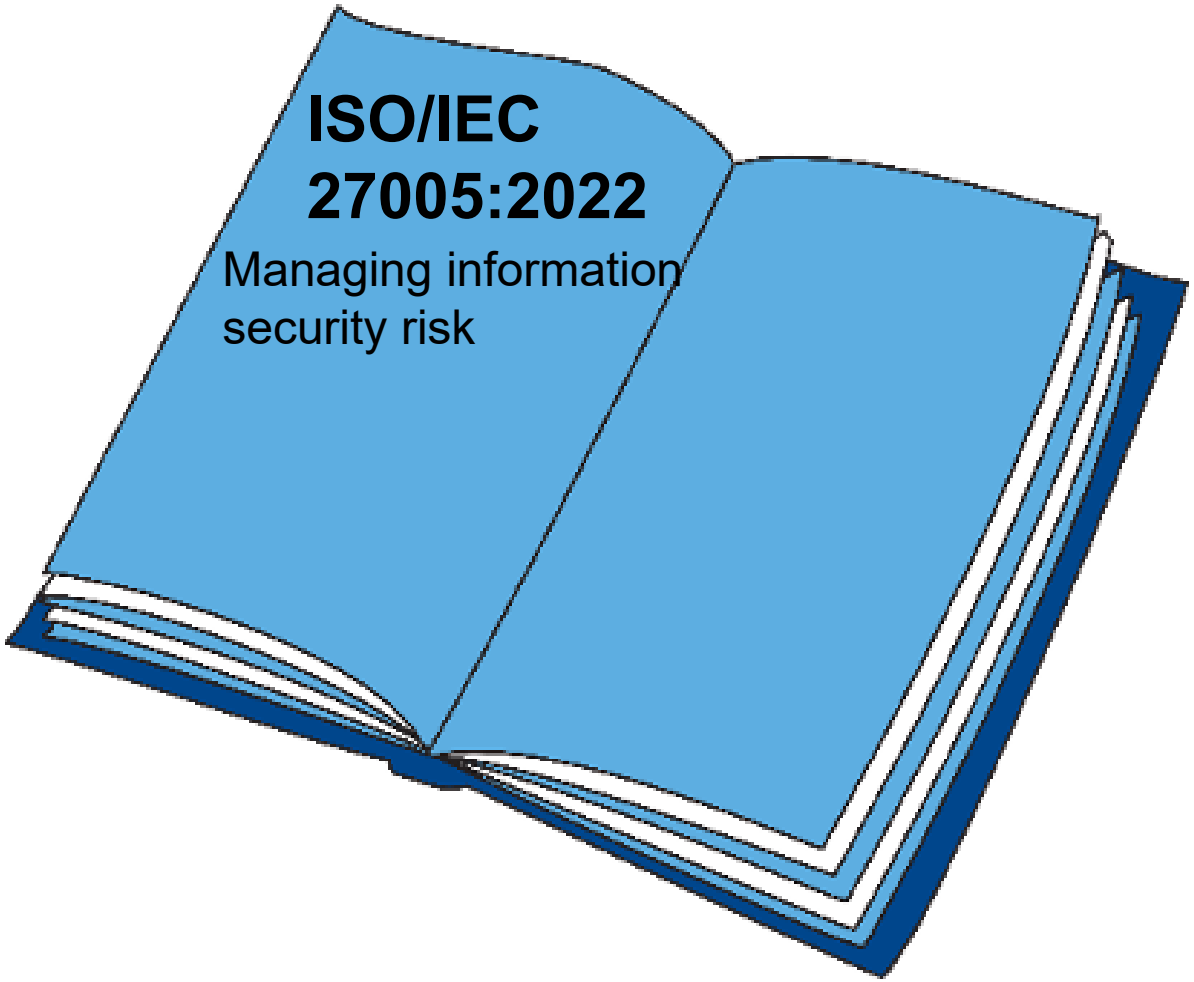
Dinh Uy Tran, Sigrid Haug Selnes, Audun Jøsang and Janne Hagen
Ph.D. candiate / Special Adviser

28.09-2023, The Hague Netherlands

Outline

- Finding/Motivation
- Research questions
- Method
- Results
- Sample case
- Conclusion

Finding/Motivation



Definition of Risk:

"the effect of uncertainty on objectives"

Positive risk

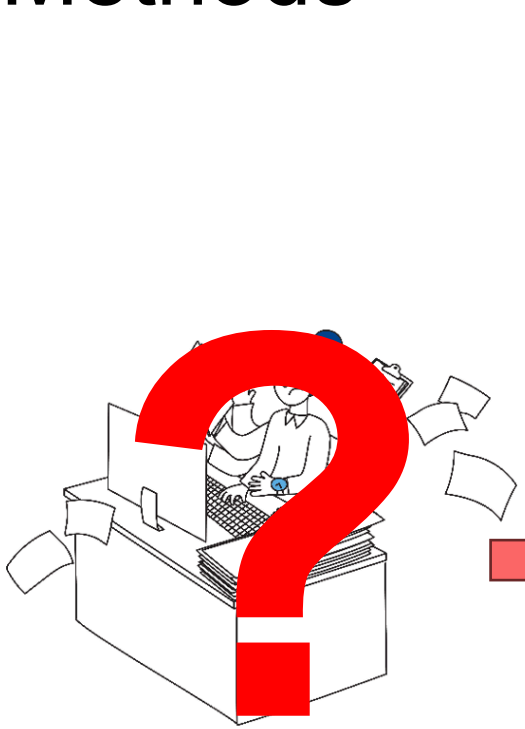
Research questions

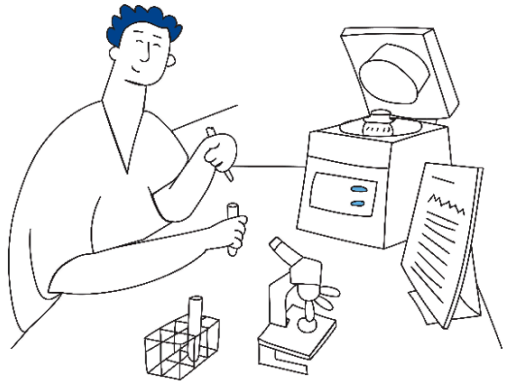
1. How should practitioners interpret the concept of risk as defined in ISO/IEC 27005:2022 to make it more applicable to both positive and negative risks?

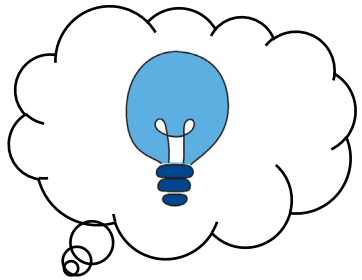
2. What should a definition of positive risk be articulated?

3. How can the definition of risk be applied to describe and assess both positive and negative risks?

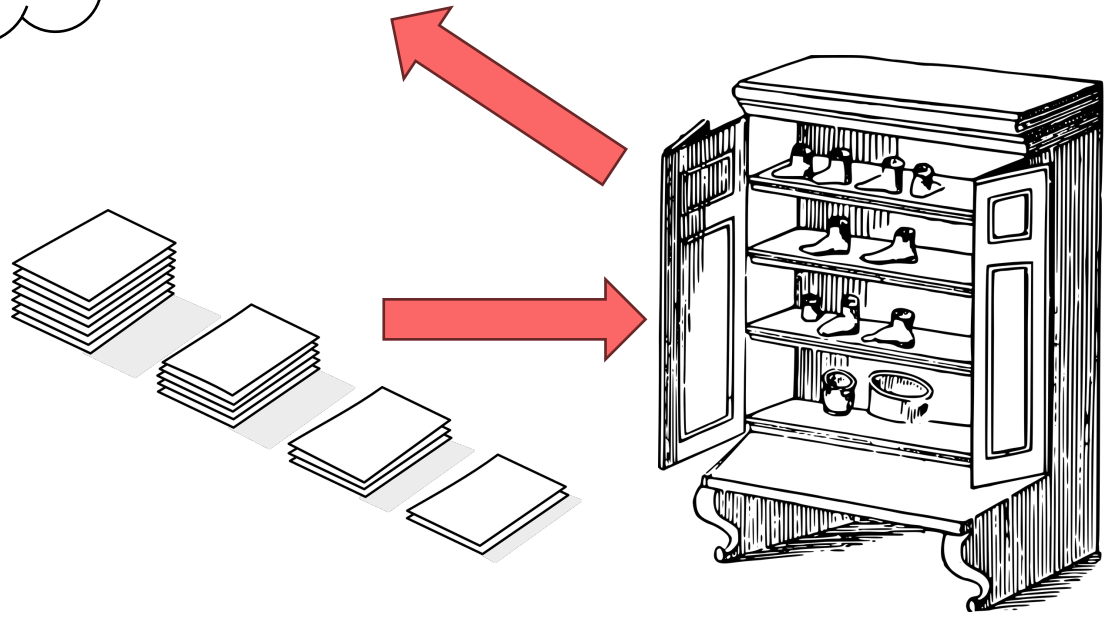
Methods







Generate new theory



www.pixabay.com

www.pixabay.com

Systematic literature review

Grounded theory

Coding and sorting

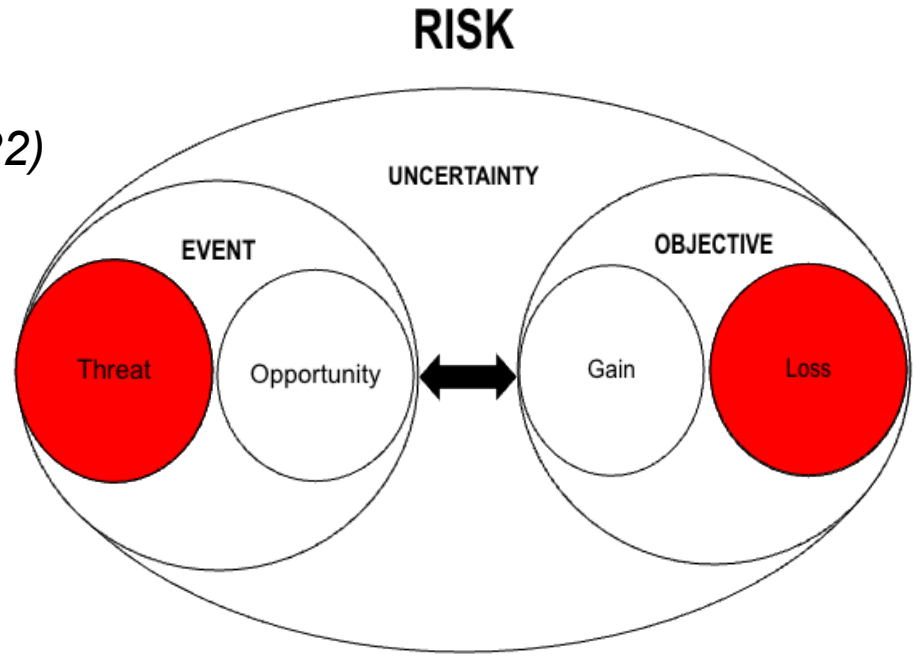
Categorisation and axial coding

Results – 1. How should practitioners interpret the concept of risk as defined in ISO/IEC 27005:2022 to make it more applicable to both positive and negative risks?

1. Tier *The effect of uncertainty on objectives (ISO/IEC 27005:2022)*

2. Tier ***"An information security risk is a possible security-related event that could affect business objectives."***

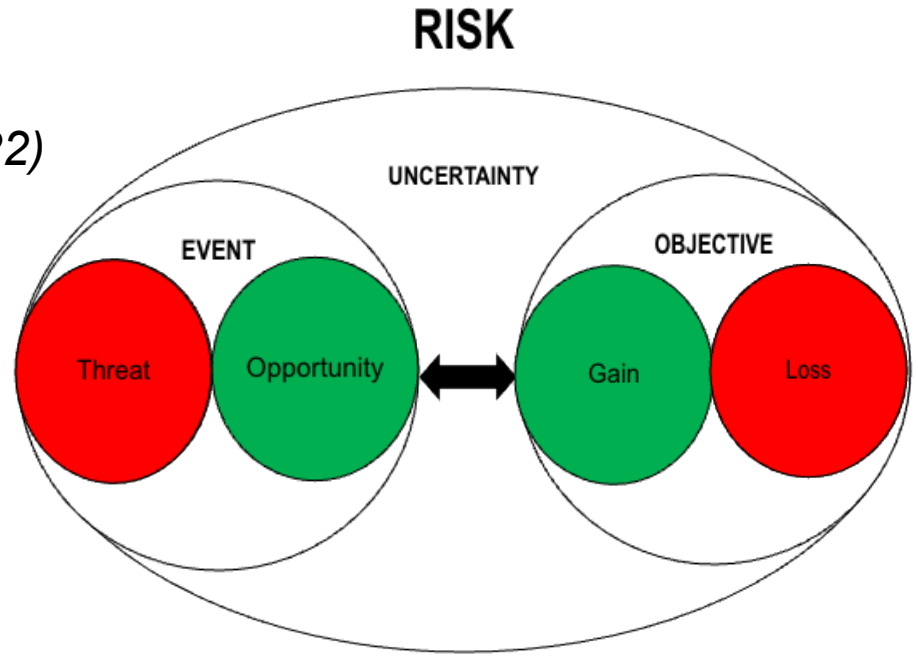
3. Tier Risk is the potential that a given threat will exploit vulnerabilities of assets and thereby cause harm to the organization *(ISO/IEC 27005:2018)*



Results – 2. What should a definition of positive risk be articulated?

1. Tier *The effect of uncertainty on objectives (ISO/IEC 27005:2022)*

2. Tier ***"An information security risk is a possible security-related event that could affect business objectives."***

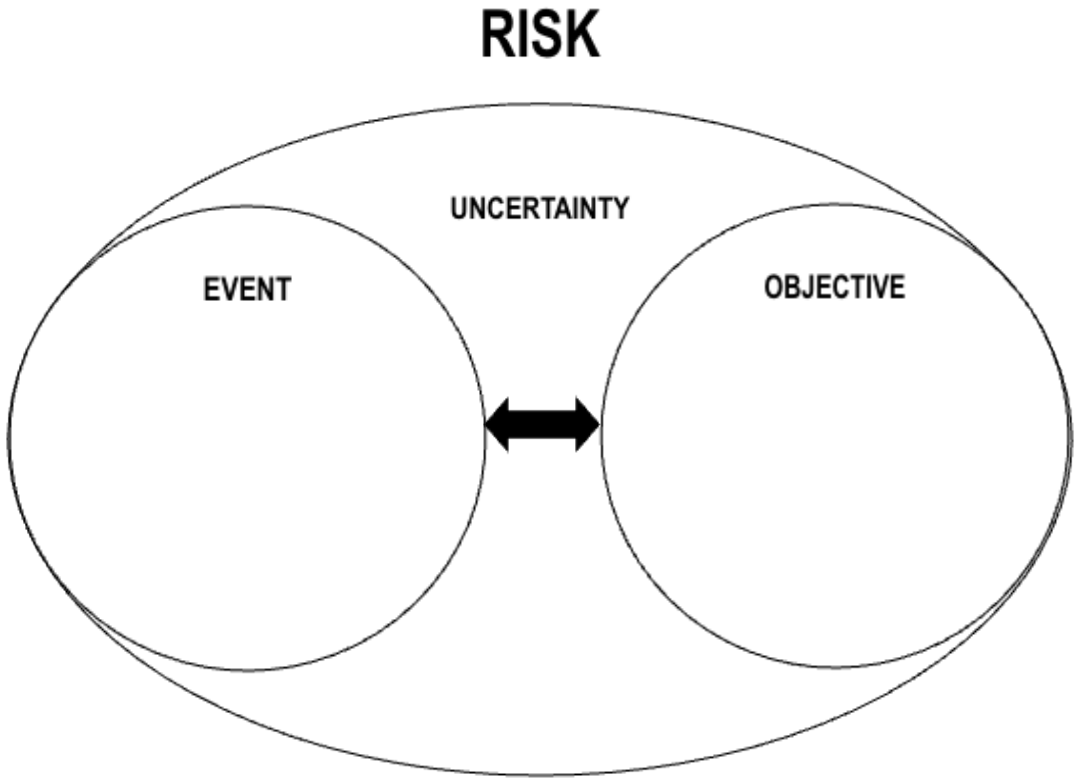


3. Tier Risk is the potential that a given threat will exploit vulnerabilities of assets and thereby cause harm to the organization *(ISO/IEC 27005:2018)*

"A positive information security risk is a possible security-related opportunity that could help businesses achieve their business objectives."

Results – 3. How can the definition of risk be applied to describe and assess both positive and negative risks?

Results – 3.1 How to describe ~~positive~~ and ~~negative~~ risk?



"An information security risk is a possible security-related event that could affect business objectives."

"There is a possibility that <insert event> could result in <insert outcome>"

Results – 3.1 How to describe positive and negative risk?

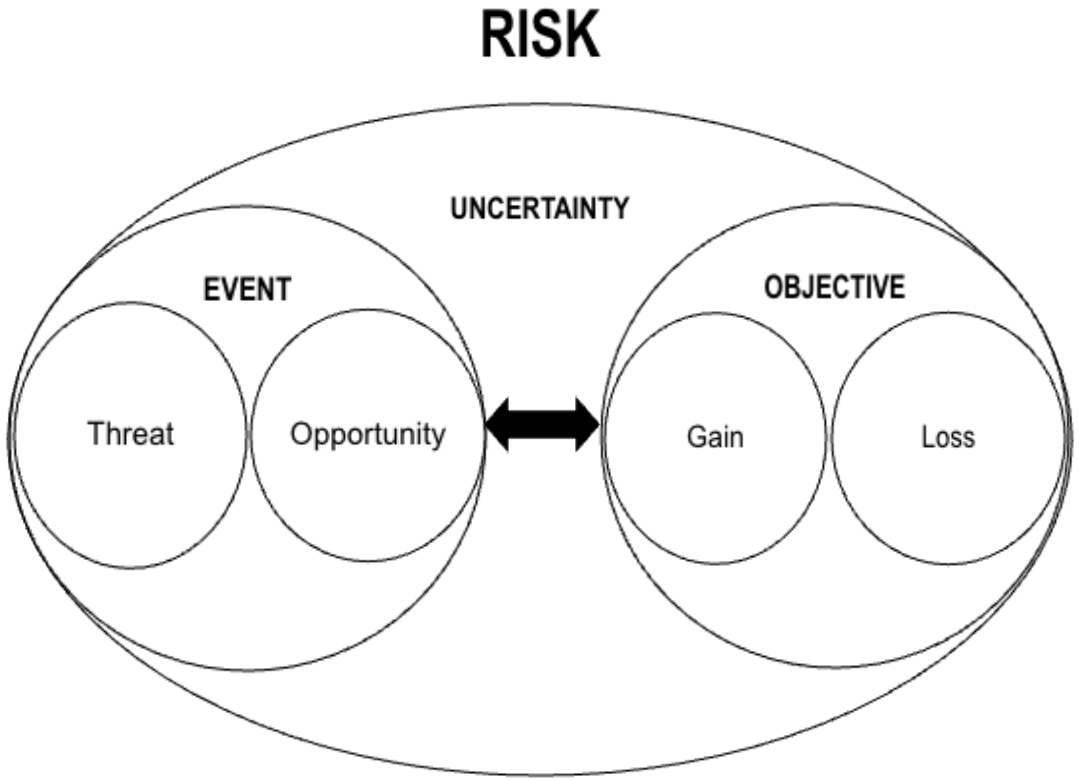


Table 2. Risk description strategies.

Alternative	Risk description alternatives
1.	There is a possibility that <insert threat> could result in <insert loss>
2.	There is a possibility that <insert threat> could result in <insert gain>
3.	There is a possibility that <insert opportunity> could result in <insert loss>
4.	There is a possibility that <insert opportunity> could result in <insert gain>

Results – 3.1 How to describe positive and negative risk?

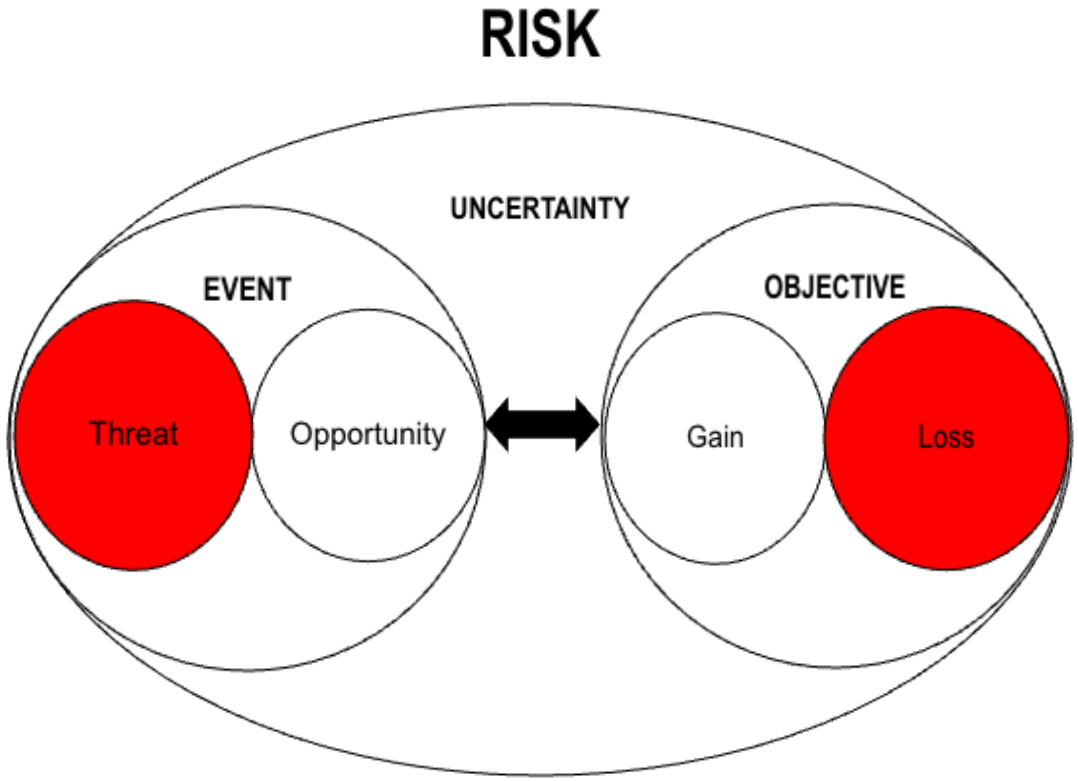


Table 2. Risk description strategies.

Alternative	Risk description alternatives
1.	There is a possibility that <insert threat> could result in <insert loss>
2.	There is a possibility that <insert threat> could result in <insert gain>
3.	There is a possibility that <insert opportunity> could result in <insert loss>
4.	There is a possibility that <insert opportunity> could result in <insert gain>

Results – 3.1 How to describe positive and negative risk?

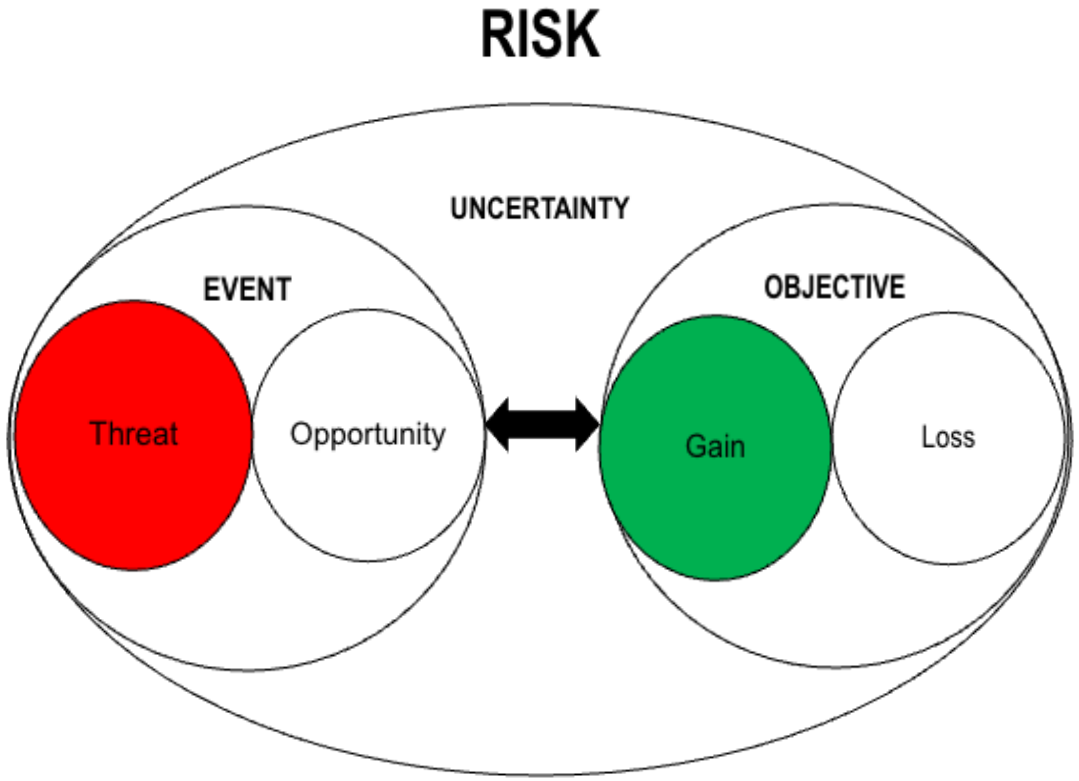


Table 2. Risk description strategies.

Alternative	Risk description alternatives
1.	There is a possibility that <insert threat> could result in <insert loss>
2.	There is a possibility that <insert threat> could result in <insert gain>
3.	There is a possibility that <insert opportunity> could result in <insert loss>
4.	There is a possibility that <insert opportunity> could result in <insert gain>

Results – 3.1 How to describe positive and negative risk?

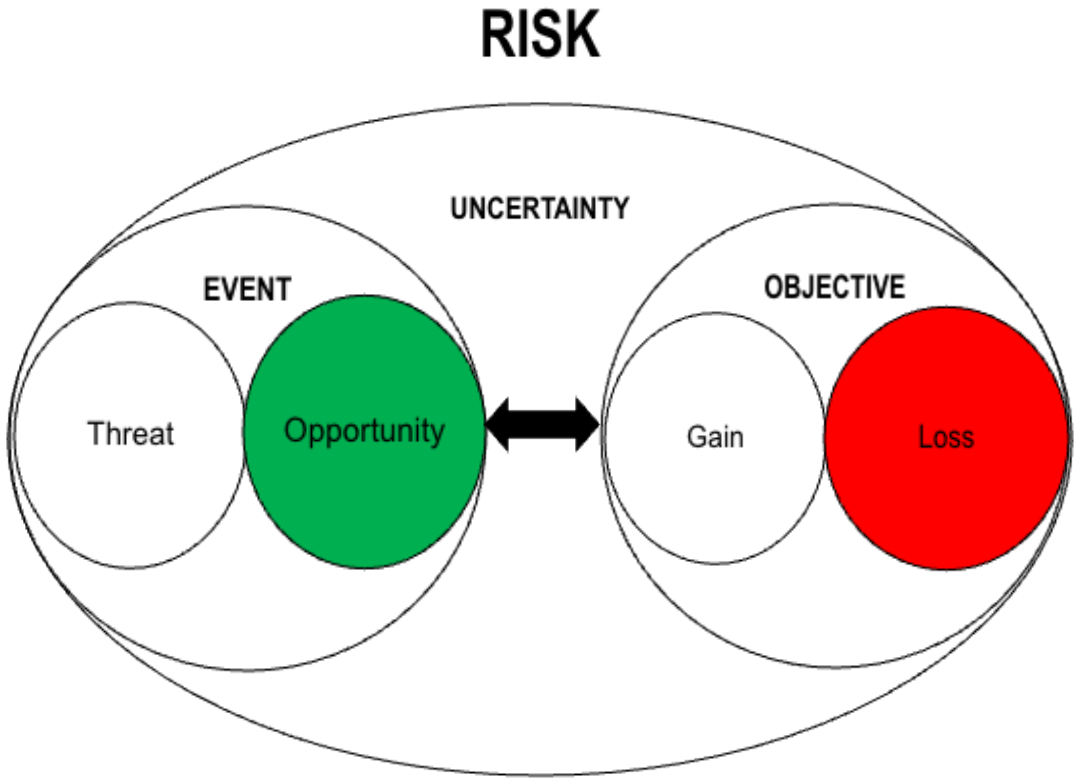


Table 2. Risk description strategies.

Alternative	Risk description alternatives
1.	There is a possibility that <insert threat> could result in <insert loss>
2.	There is a possibility that <insert threat> could result in <insert gain>
3.	There is a possibility that <insert opportunity> could result in <insert loss>
4.	There is a possibility that <insert opportunity> could result in <insert gain>

Results – 3.1 How to describe positive and negative risk?

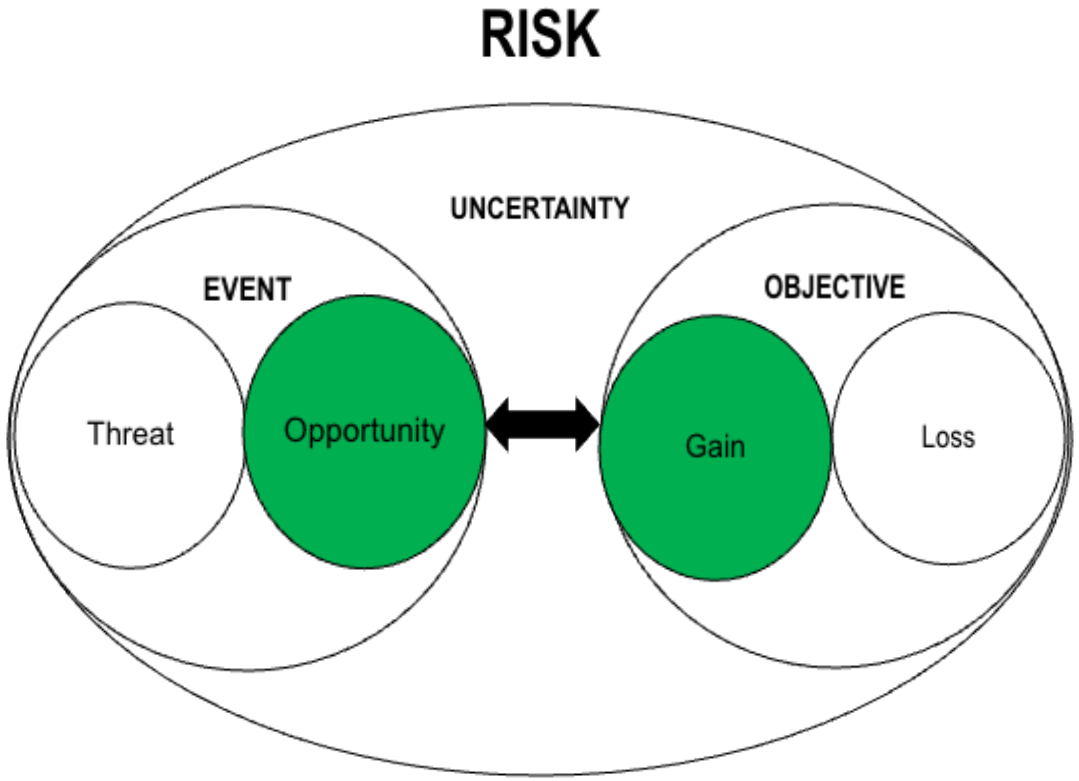


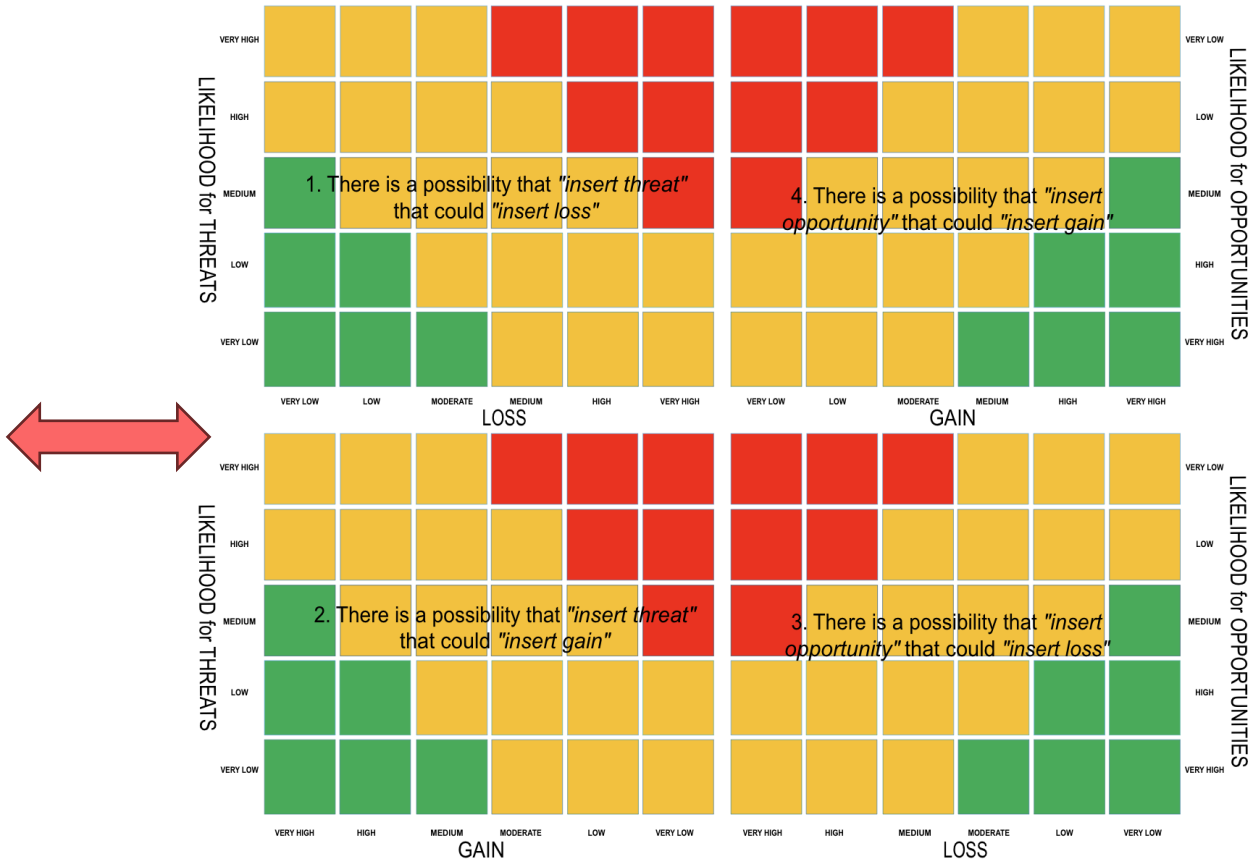
Table 2. Risk description strategies.

Alternative	Risk description alternatives
1.	There is a possibility that <insert threat> could result in <insert loss>
2.	There is a possibility that <insert threat> could result in <insert gain>
3.	There is a possibility that <insert opportunity> could result in <insert loss>
4.	There is a possibility that <insert opportunity> could result in <insert gain>

Results – 3.2 How to assess positive and negative risks?

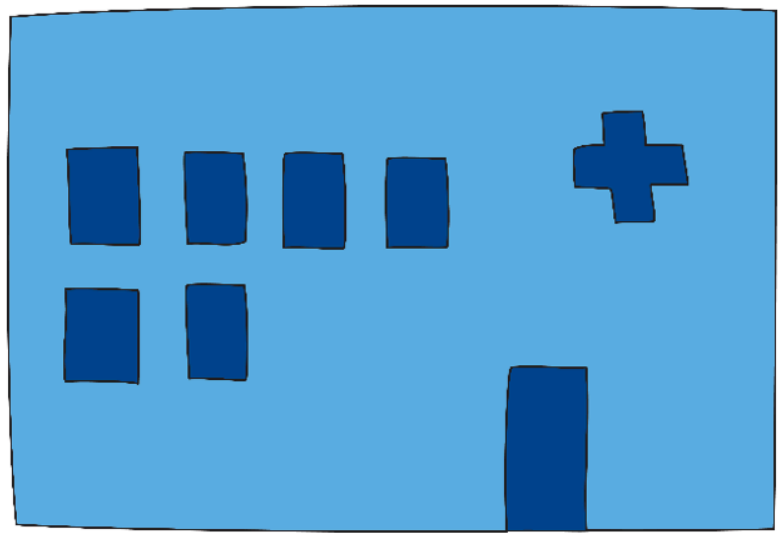
Table 2. Risk description strategies.

Alternative	Risk description alternatives
1.	There is a possibility that <insert threat> could result in <insert loss>
2.	There is a possibility that <insert threat> could result in <insert gain>
3.	There is a possibility that <insert opportunity> could result in <insert loss>
4.	There is a possibility that <insert opportunity> could result in <insert gain>

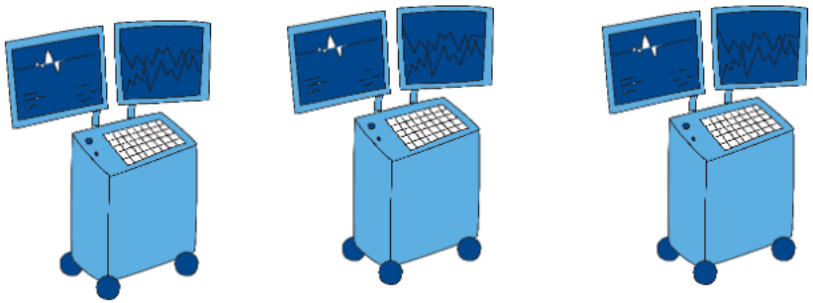


Sample case – Emergency healthcare

- Purpose
  - Doctors rely on advanced technology to perform emergency health care procedures
  - Lately some technical issues
  - Hired a risk analyst to get a better understanding of risk related to information security

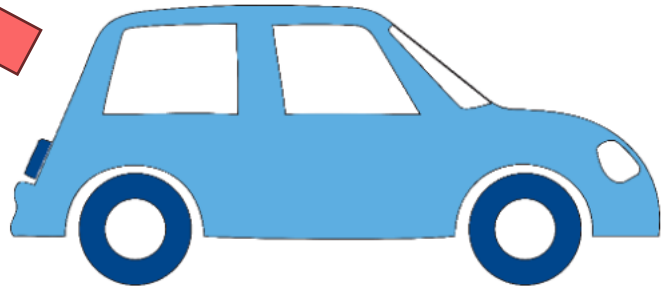


Findings



The same system is installed locally on different equipments

Travel time: 30 minutes

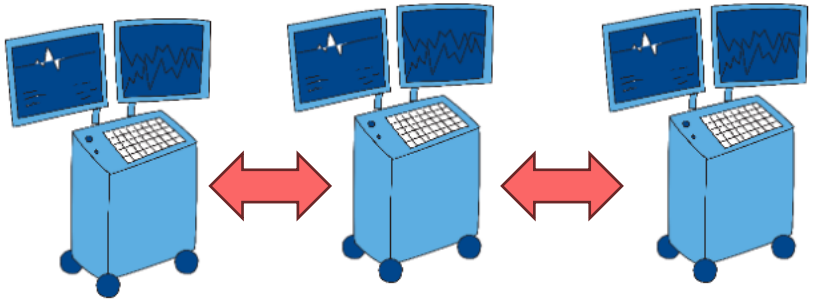


Staff must be on-site to the fix issue

Solution

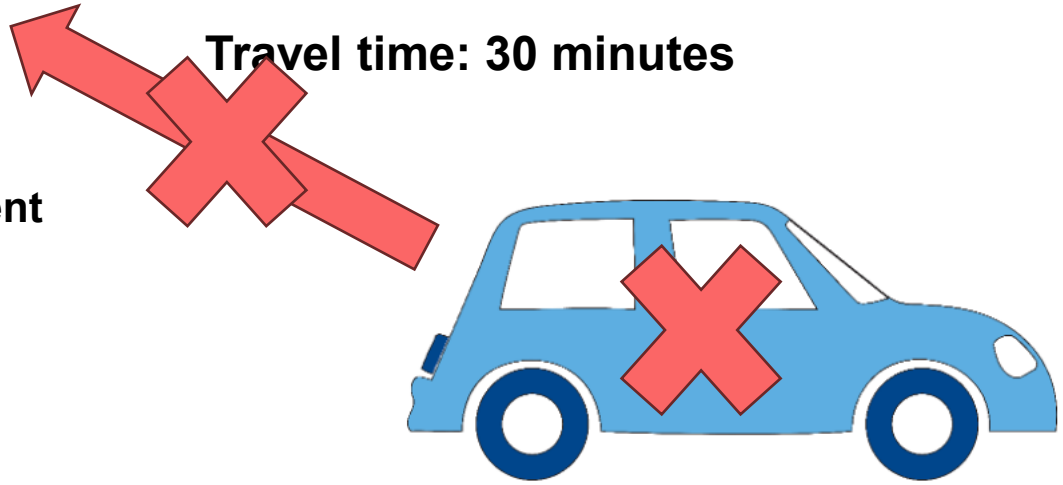
Centralized

Monitoring



The same system is installed locally on different equipments

Travel time: 30 minutes



Staff must be on-site to fix the issue

Risk description alternative 1

Threat

“There is a possibility **that malware can be installed without detection**, which could **cause business disruption.**”

Loss

Who?: Top-level management and Security staff

Likelihood: Very high, lack of monitoring tools

Impact: Very high, not centralized and time consuming

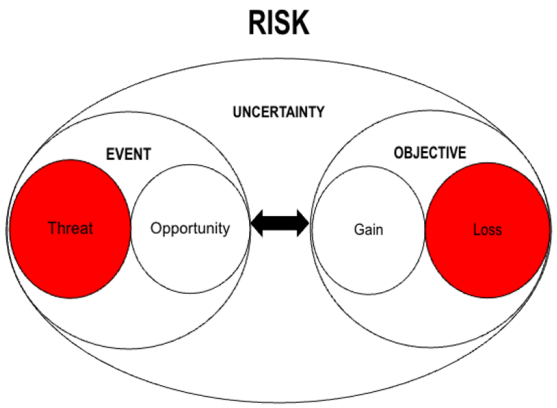
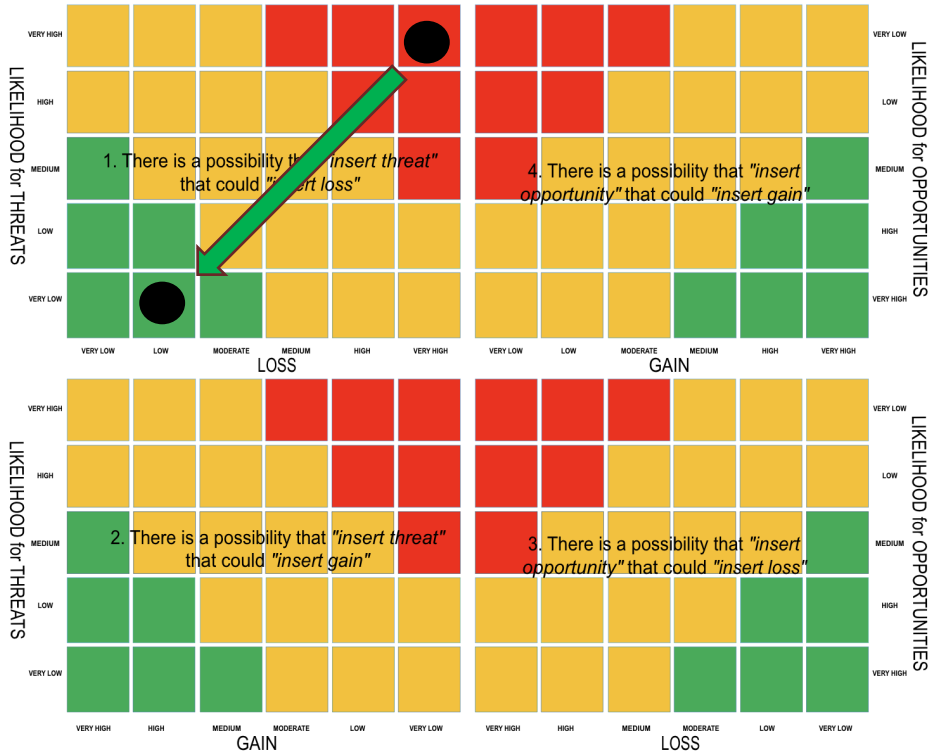


Table 2. Risk description strategies.

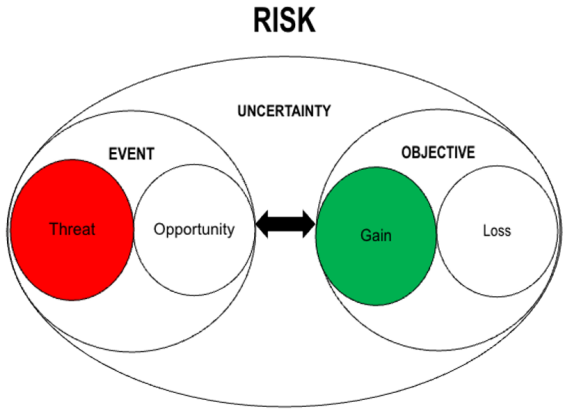
Alternative	Risk description alternatives
1.	There is a possibility that <insert threat> could result in <insert loss>
2.	There is a possibility that <insert threat> could result in <insert gain>
3.	There is a possibility that <insert opportunity> could result in <insert loss>
4.	There is a possibility that <insert opportunity> could result in <insert gain>



UNIVERSITY OF OSLO

SYKEHUSPARTNER

Risk description alternative 2



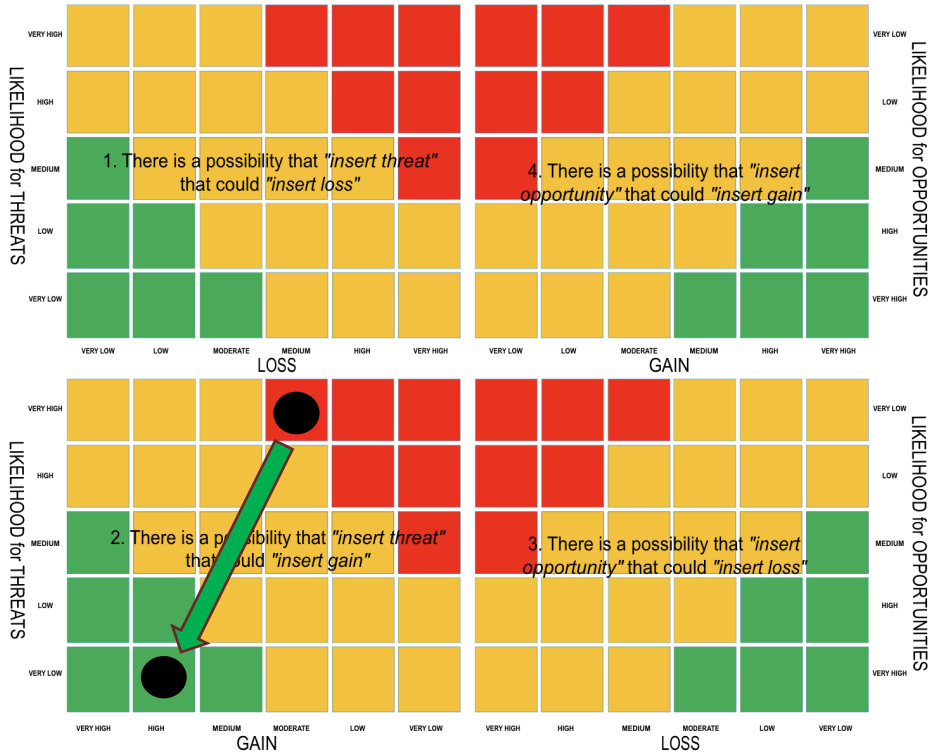
Threat

”There is a possibility **that malware can be installed without detection**, which would **not cause any business disruption**.”

Gain

Table 2. Risk description strategies.

Alternative	Risk description alternatives
1.	There is a possibility that <insert threat> could result in <insert loss>
2.	There is a possibility that <insert threat> could result in <insert gain>
3.	There is a possibility that <insert opportunity> could result in <insert loss>
4.	There is a possibility that <insert opportunity> could result in <insert gain>



Who?: Security and IT staff

Likelihood: Very high, lack of monitoring tools

Impact: Medium, Experienced IRT team

UNIVERSITY OF OSLO

SYKEHUSPARTNER

Risk description alternative 3

Opportunity

”There is a possibility that **acquiring updated infrastructure (centralised, monitoring capabilities)** could **cause business disruption**.”

Loss

Who?: All stakeholder who prefer solutions

Likelihood: Depends on aquisition and project management skills

Impact: Depends on ICT architecture skills and IRT

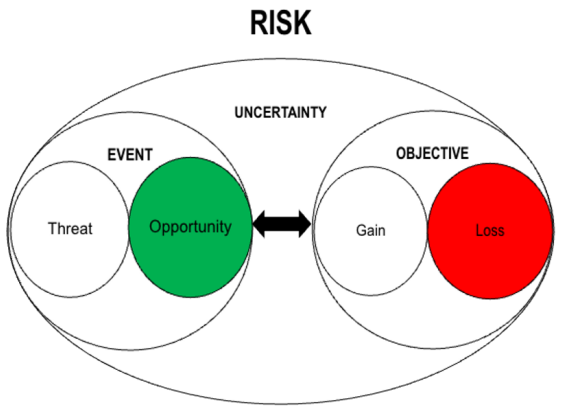
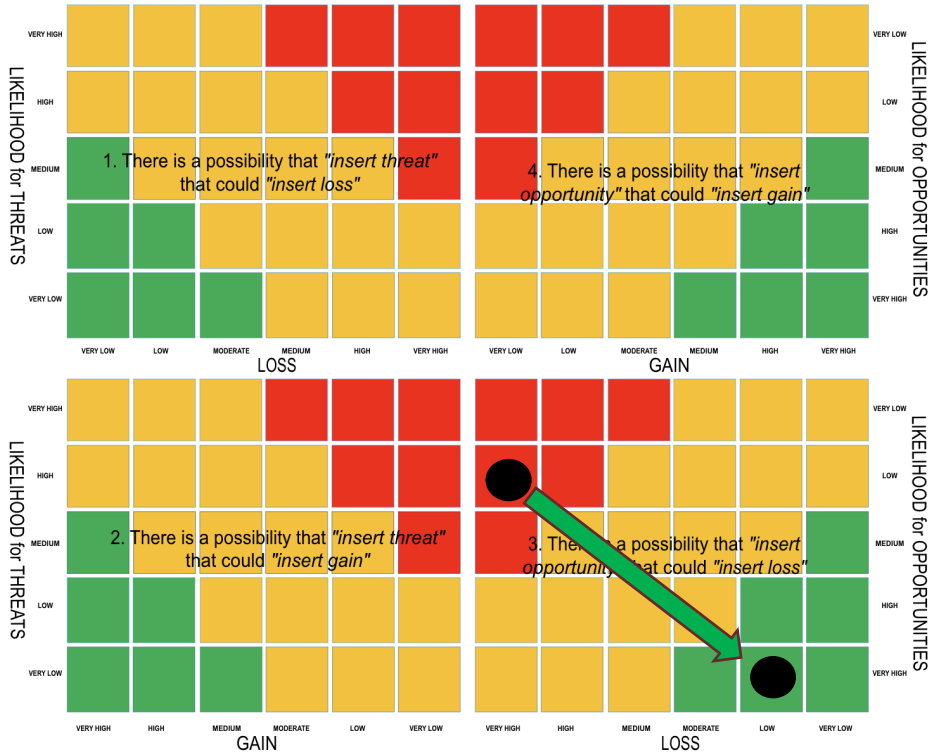


Table 2. Risk description strategies.

Alternative	Risk description alternatives
1.	There is a possibility that <insert threat> could result in <insert loss>
2.	There is a possibility that <insert threat> could result in <insert gain>
3.	There is a possibility that <insert opportunity> could result in <insert loss>
4.	There is a possibility that <insert opportunity> could result in <insert gain>



UNIVERSITY OF OSLO

SYKEHUSPARTNER

Risk description alternative 4

Opportunity

”There is a possibility that **acquiring updated infrastructure detection of faults in the system(centralised, monitoring capabilities)**
could **reduce the workload of the IT and security staff, and give a more reliable system**.”

Gain

Who?: All stakeholder who prefer solutions

Likelihood: Depends on aquisition and project management skills

Impact: Depends on ICT architecture skills and involvement of staff

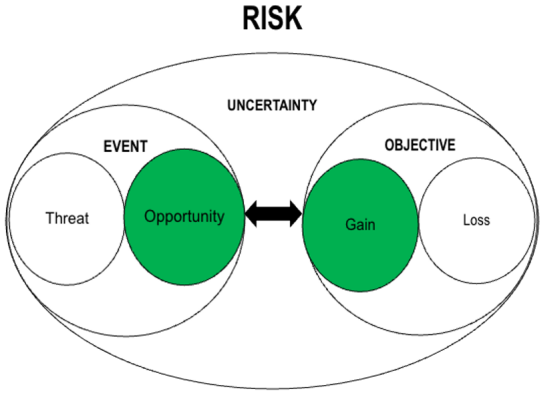
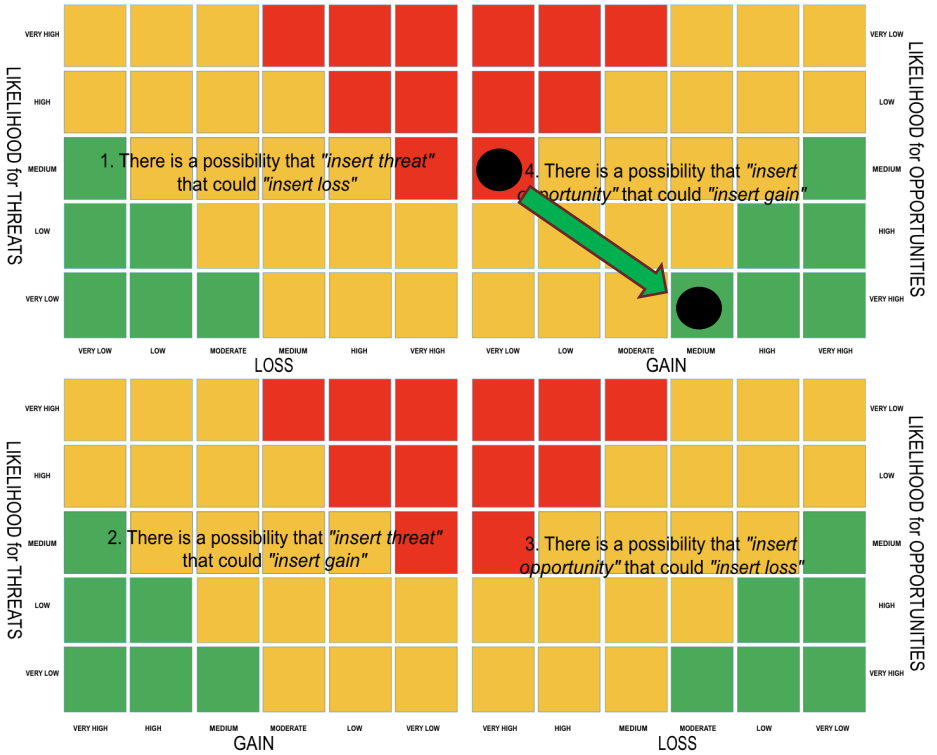


Table 2. Risk description strategies.

Alternative	Risk description alternatives
1.	There is a possibility that <insert threat> could result in <insert loss>
2.	There is a possibility that <insert threat> could result in <insert gain>
3.	There is a possibility that <insert opportunity> could result in <insert loss>
4.	There is a possibility that <insert opportunity> could result in <insert gain>



UNIVERSITY OF OSLO

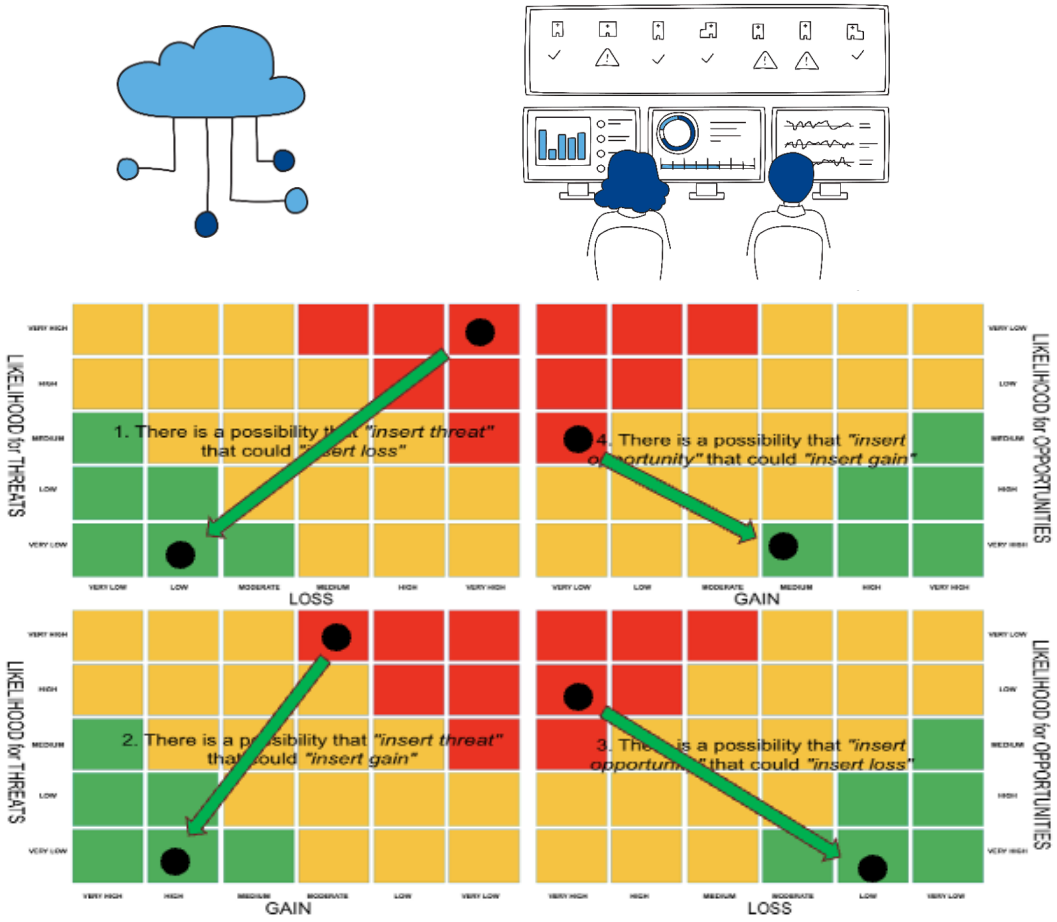
SYKEHUSPARTNER

Summary

-Same solutions but different strategies

-Management of positive and negative risk

-Apply security measures to ensure residual risk is at an acceptable level



UNIVERSITY OF OSLO

SYKEHUSPARTNER

Conclusion

- Contributions
  - Proposed an updated definiton of risk
  - Proposed a new definiton of positive risk
  - Conceptualisation of risk
  - Risk decription strategies
  - Four dimensional risk matrix
- Future leaders might expect security professionals to manage positive risk
- We need to adapt to a business-oriented approach!

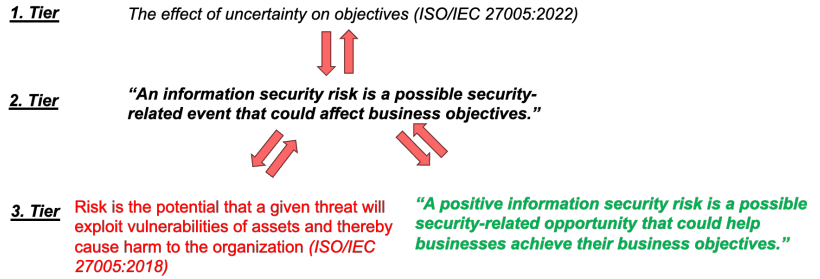
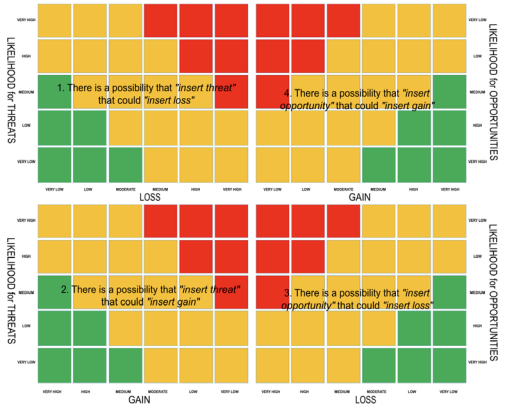


Table 2. Risk description strategies.

Alternative	Risk description alternatives
1.	There is a possibility that <insert threat> could result in <insert loss>
2.	There is a possibility that <insert threat> could result in <insert gain>
3.	There is a possibility that <insert opportunity> could result in <insert loss>
4.	There is a possibility that <insert opportunity> could result in <insert gain>



Thank you for your attention!

Contact information

- E-mail: dinhut@ifi.uio.no
- Linkedin: www.linkedin.com/in/uydinhtran
- Homepage: https://www.mn.uio.no/ifi/english/people/aca/dinhut/index.html