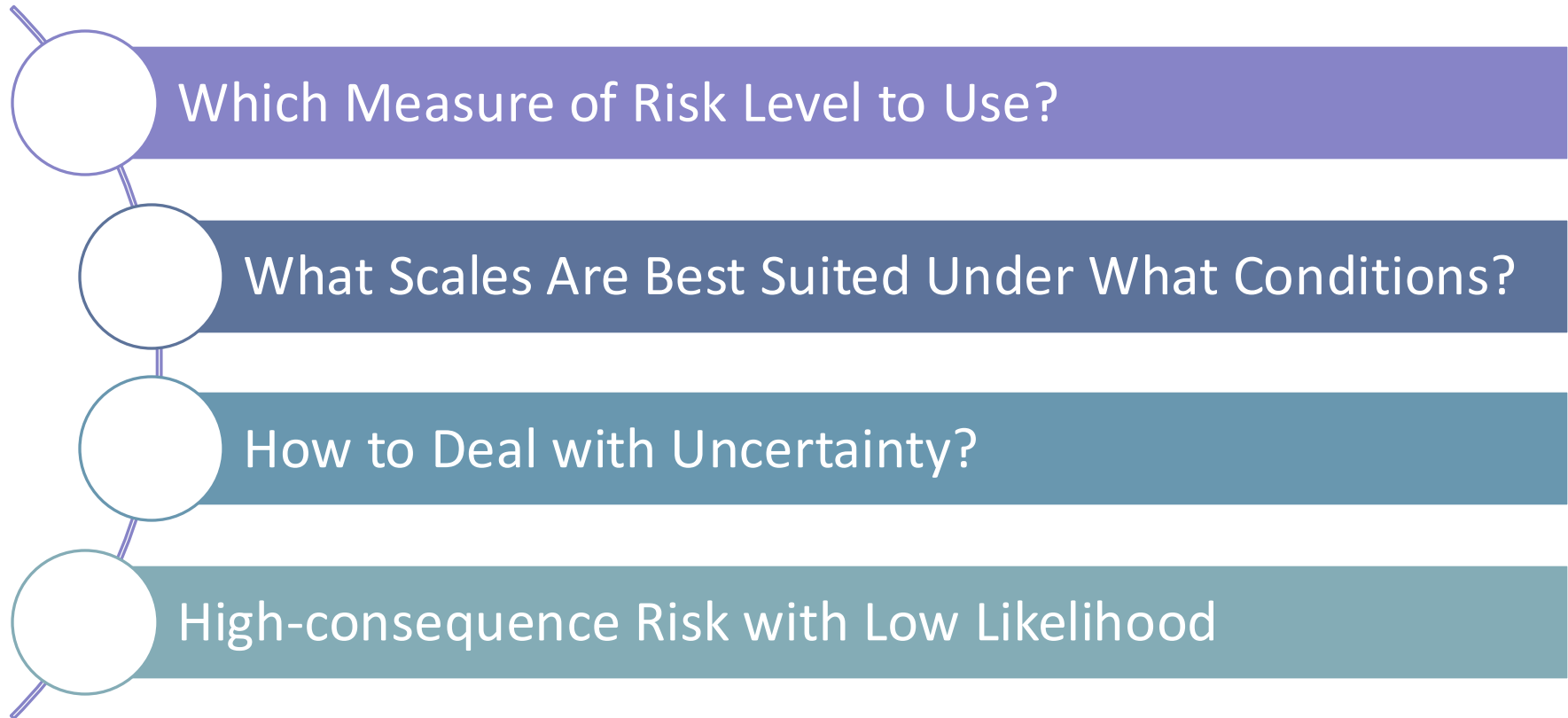


Security Governance Master of Science in Cyber Security

AA 2024/2025

RISK MANAGEMENT: CHALLENGES AND GUIDELINES

Challenges in the Cyber-Risk Management process

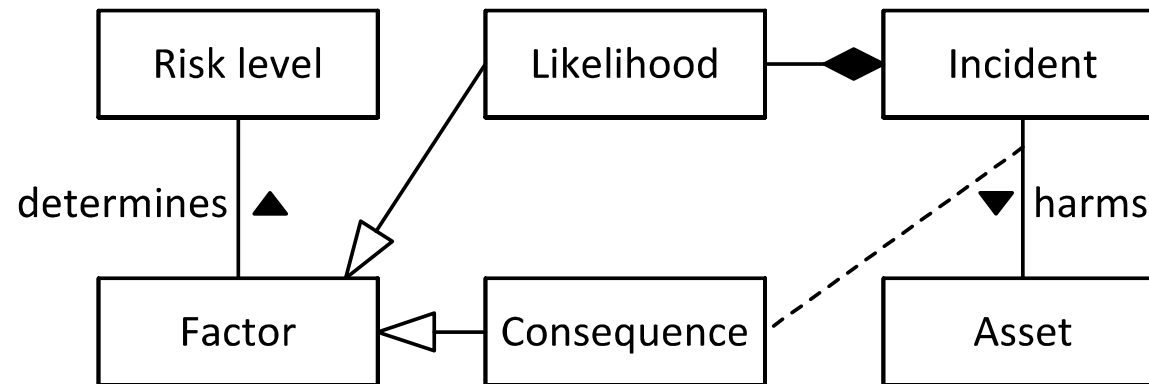


Which Measure of Risk Level to Use?

Up to now, we measured risk level based on two factors:

- loss of asset value when a potential incident occurs (i.e., consequences)
- how often this happens (i.e., likelihood)

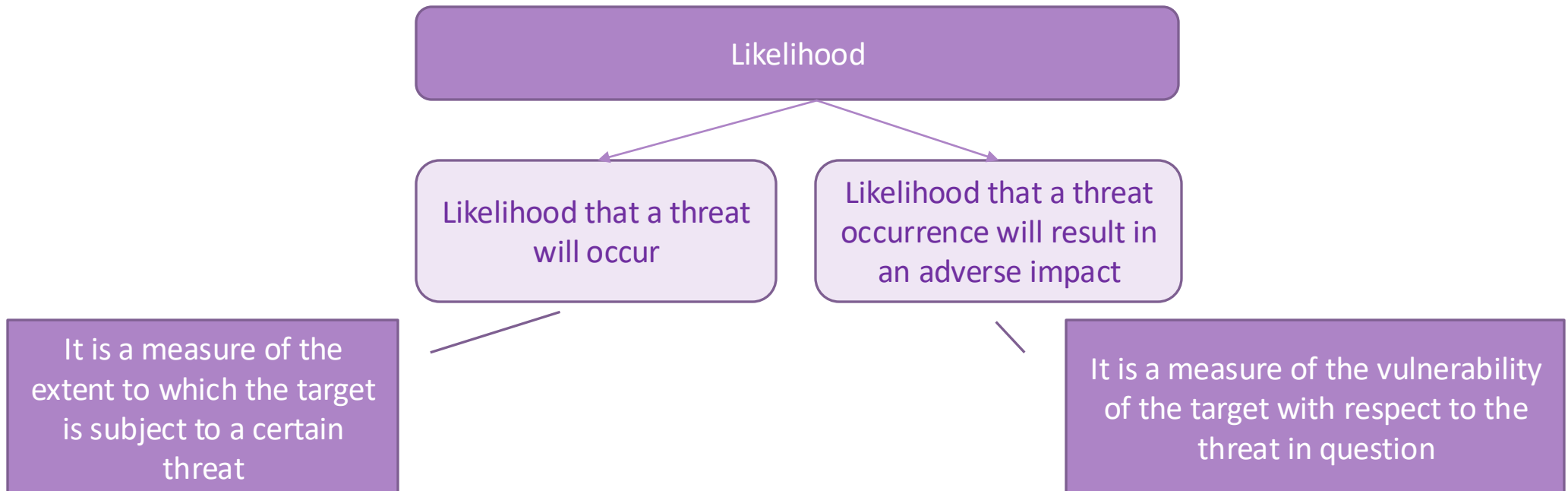
This is a classical two-factor measure of risk



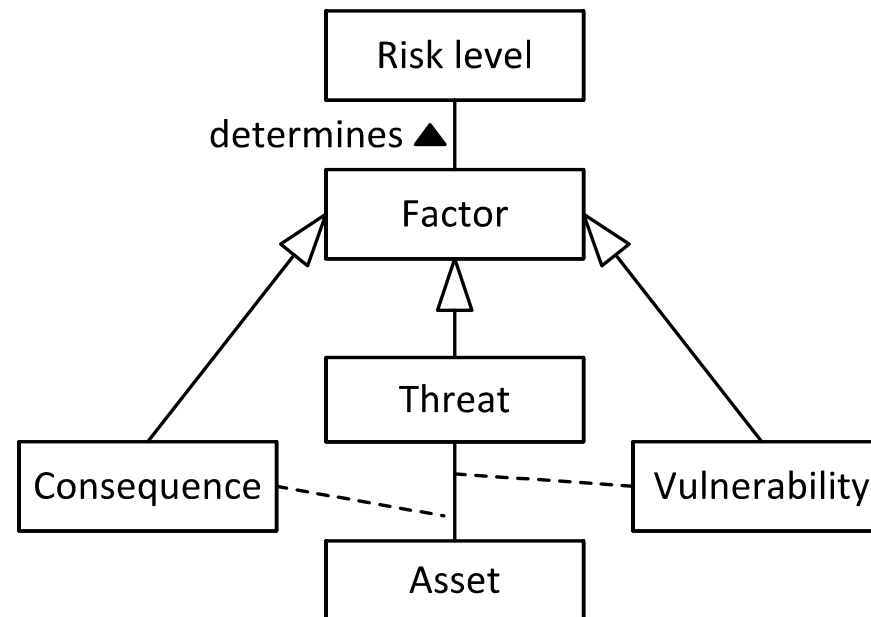
Three-factor Measure

NIACAP defines risk as

“a combination of the likelihood that a threat will occur, the likelihood that a threat occurrence will result in an adverse impact, and the severity of the resulting impact”



Three-factor Measure



Many-factor Measure

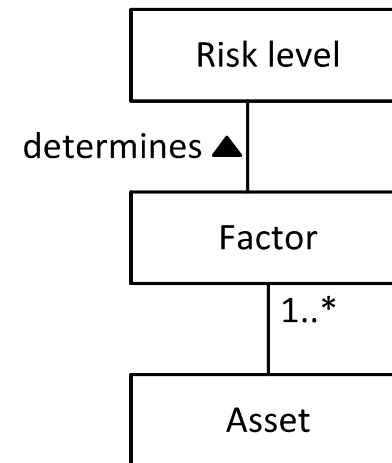
In some methodologies (e.g., OWASP) threats and vulnerabilities are analysed under different factors

Such factors may be considered independently as factors affecting the risk level

- threat agent factors
- vulnerability factors

Similarly, consequence is represented by

- technical impact factors
- business impact factors



Which Measure to Use for Cyber-risk?

Which approach you should use and how you should use it depends on the context and your risk assessment situation

Considerations

- data availability is an important parameter when deciding how to measure risk level
 - If you have good data on frequency and consequence you will probably go for the two-factor approach
- Within cybersecurity the popularity of multi-factor measures is growing
 - measuring likelihood with a reasonable degree of uncertainty in practice may be difficult

Which Measure to Use for Cyber-risk?

Which approach you should use and how you should use it depends on the context and your risk assessment situation

Considerations

- When assessing risk, the problem is not the lack of data, but the lack of the right kind of data with respect to predefined factors
 - Most cyber-systems generate logs automatically with respect to a (large) number of indicators
 - In such situations you may try to define your own risk function from factors matching the indicators logged by the cyber-system in question
 - **WARNING**: it requires some experience and great care

Which Measure to Use for Cyber-risk?

Which approach you should use and how you should use it depends on the context and your risk assessment situation

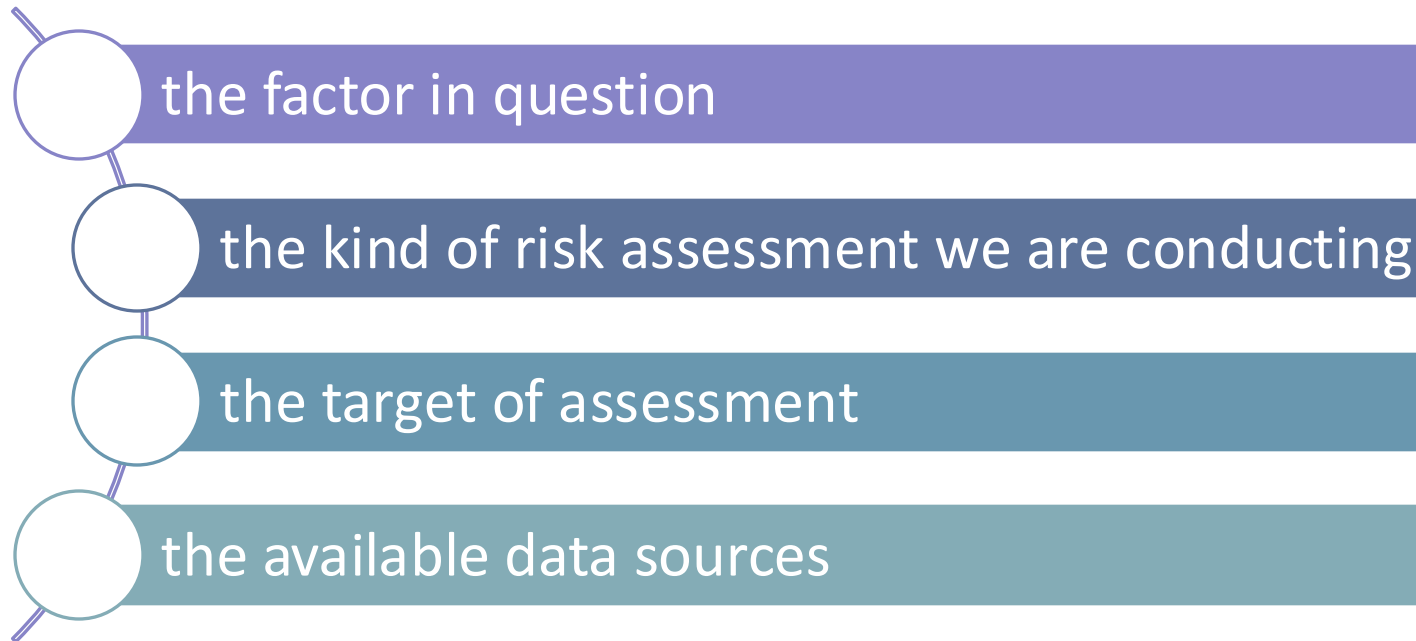
Considerations

- If you rely on expert or stakeholder opinions to estimate risk level, make sure that the factors are carefully defined and easy to keep apart
- It is also crucial that you select the right kind of scale for each factor

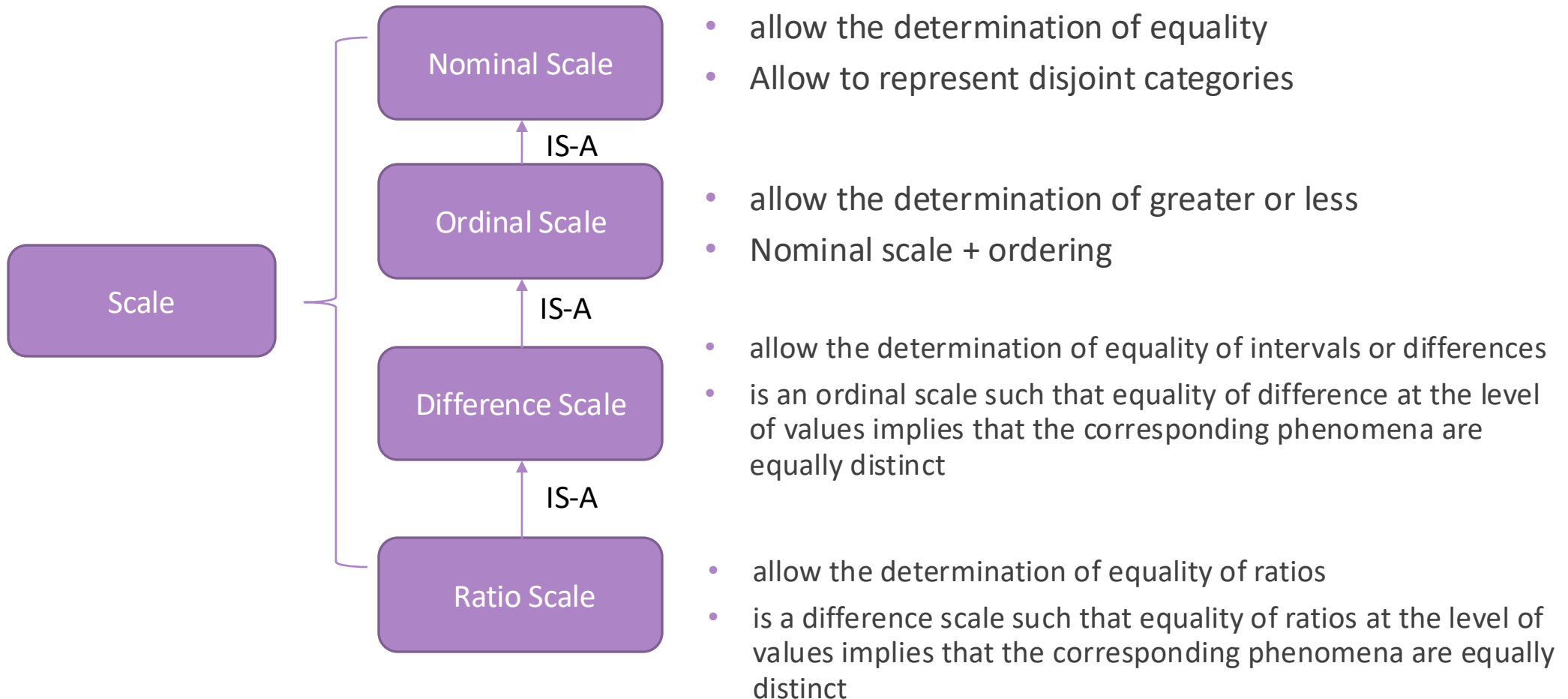
What Scales Are Best Suited Under What Conditions?

Observation

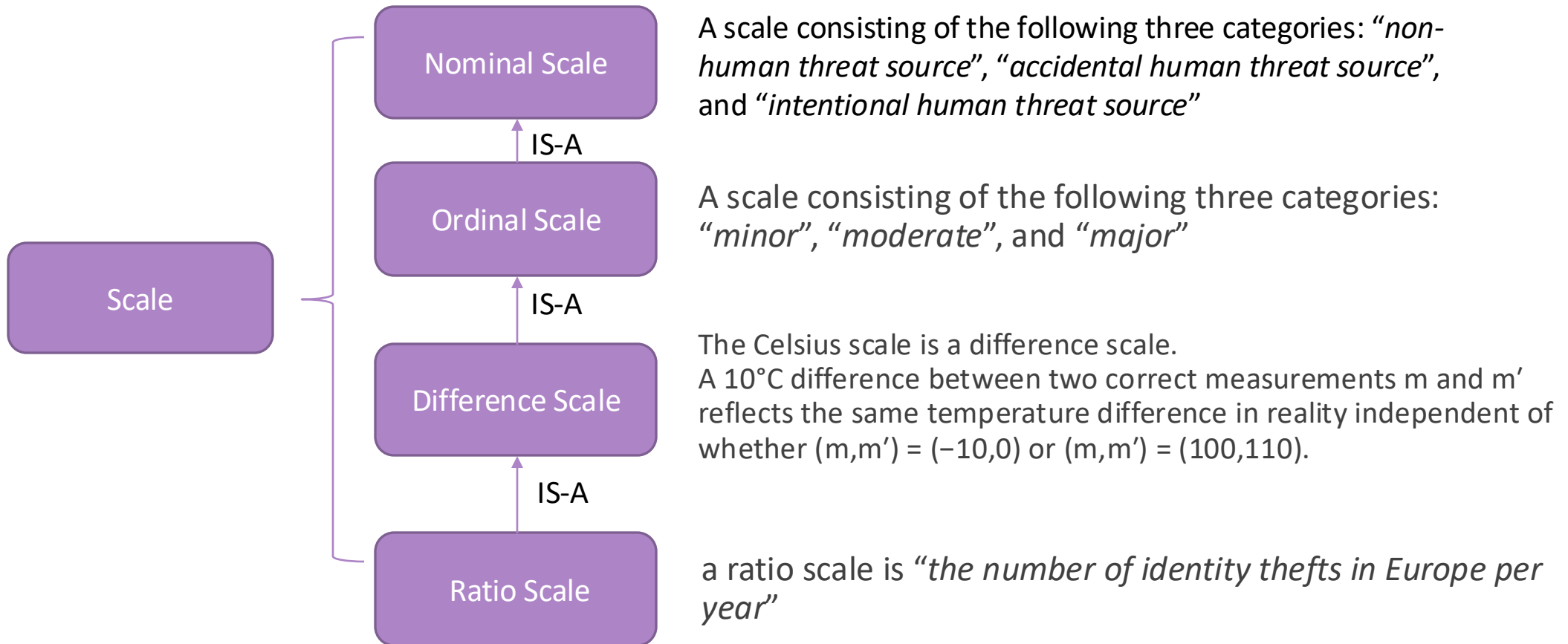
The suitability of a scale depends on

- 
- the factor in question
 - the kind of risk assessment we are conducting
 - the target of assessment
 - the available data sources

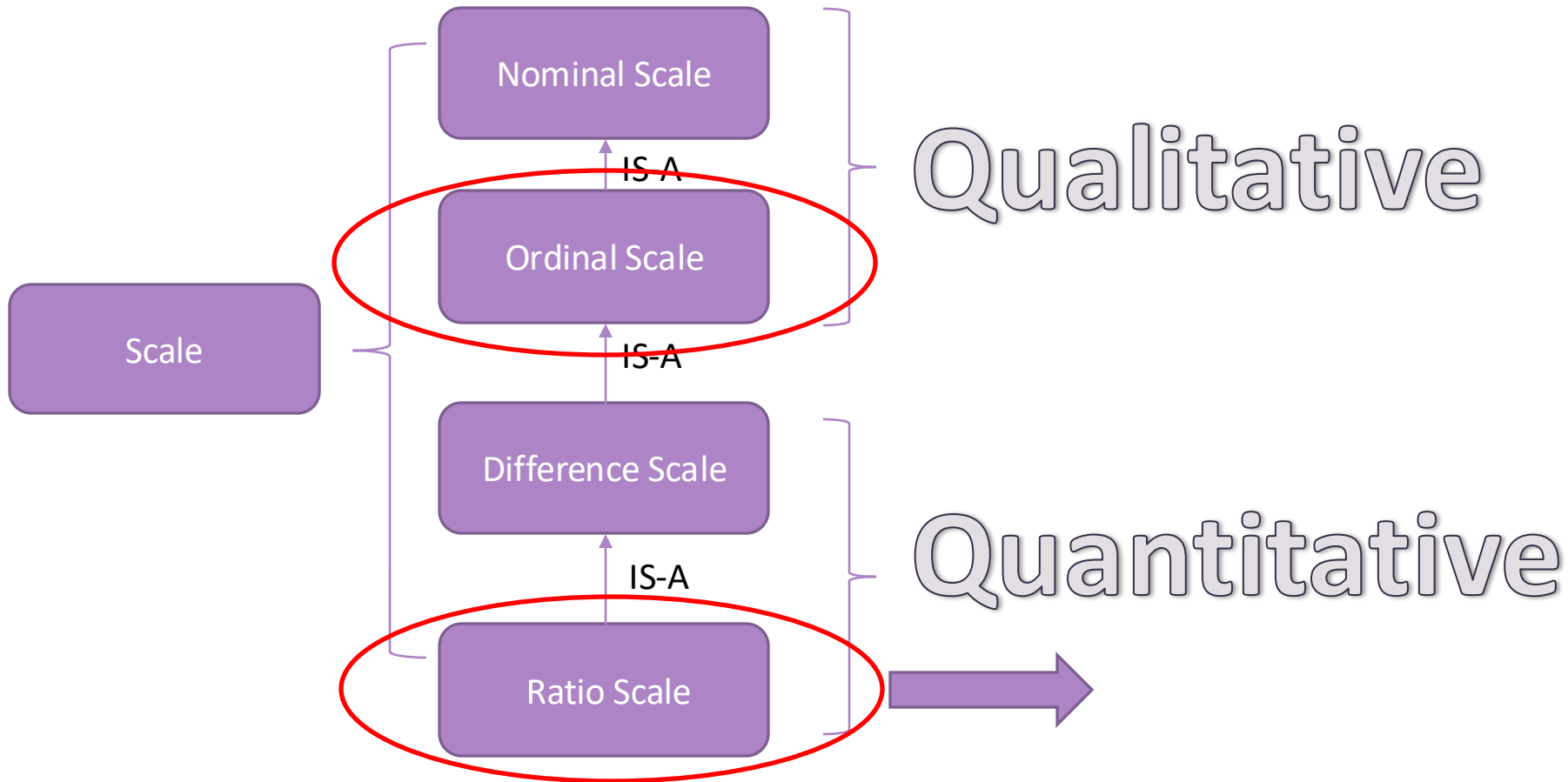
Classification of Scales



Classification of Scales



Classification of Scales



Qualitative Versus Quantitative Risk Assessment

QUANTITATIVE

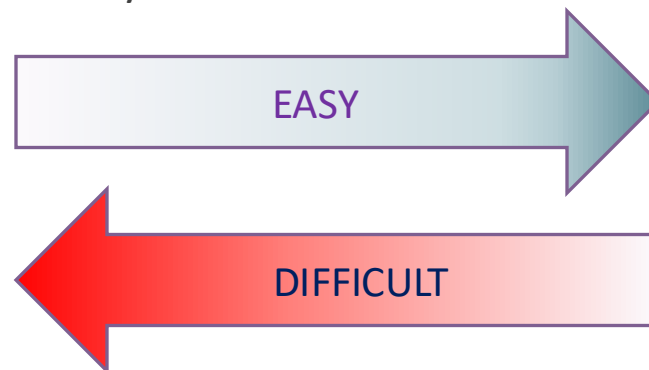
Information that need to be quantified are homogeneous

Tends to work better when

- The assessment is at a more technical level or
- It requires fine level of granularity.

QUALITATIVE

Information that need to be quantified are NOT homogeneous



Qualitative Versus Quantitative Risk Assessment

QUANTITATIVE

Working with exact quantities is fine in theory but not necessarily very practical

- Quantitative scales may yield infinitely many values of risk level, although perhaps three or five would be sufficient

QUALITATIVE

A purely qualitative approach is not satisfactory on its own

- result of any risk assessment must be converted to a quantitative scale in some way or another in the end (typically costs measured through money).

Scales for Likelihood

Estimating or measuring likelihood tends to be difficult

- there may be considerable uncertainty as to what the likelihood is
- there may be lack of experience or historical data with respect to the event in question
- bad selection of a quantitative scale that is badly suited to the task

SUGGESTIONS

- It is not recommended to use probabilities when interacting with people in a risk assessment situation
- intervals of frequencies or qualitative scales work best in practice

Scales for Consequence

A risk evaluation may end up with a cost-benefit analysis or be used as input for cost-benefit analysis

Depending on the kinds of assets to be protected, this may not work well in practice.

- **Example 1:** if the asset in question is a bag of diamonds the consequence of an incident in which some or all of the diamonds are stolen might be equal to the monetary value of the diamonds stolen
- **Example 2:** if the asset is the integrity of a customer database, it may be easy to characterize the number of records harmed, but hard to say what this means in euros
- **Example 3:** if the asset is the company's reputation, it is hard to know or characterize the impact of some incident on it, and even harder to estimate what this impact corresponds to in euros

Scales for Consequence

OBSERVATION: The suitability of a consequence scale obviously depends on the asset in question

It is recommended to:

- Define specialized consequence scales for each asset of relevance
- Define a consequence scale in such a way that it fits its intended usage
 - E.g., A consequence scale suited for communicating consequences to decision makers may be unsuited to discussions with technical people.

What Scales to Use for Cyber-risk?

The main simplifying feature is that cyber-risk concerns systems which to a large extent are computerized

- The computerized parts are well-suited for automatic measurement and logging

A complicating feature is the openness of cyberspace and the fact that it is often necessary to measure human intentions and skills.

How to Deal with Uncertainty?

ISO 31000 defines uncertainty to be
“the state, even partial, of deficiency of information related to, understanding or knowledge of an event, its consequence, or likelihood”

We will distinguish between two kinds of uncertainty:

- epistemic uncertainty
- aleatory uncertainty

We will focus on how to represent uncertainty and how to reduce it

we will address challenges related to uncertainty in the setting of cyber-risk assessment

Epistemic vs Aleatory Uncertainty

Epistemic Uncertainty relates to the uncertainty due to ignorance or lack of evidence.

- In the case of perfect knowledge there is no epistemic uncertainty.
- There is no further knowledge to be gained from additional empirical investigations
- In the case of imperfect knowledge there is always some epistemic uncertainty

Aleatory Uncertainty relates to the uncertainty due to inherent randomness

How can we Represent Uncertainty?

Using quantitative scales

- we may represent uncertainty by using intervals
- the width of the interval specifies the level of uncertainty

How much uncertainty is tolerable?

- It depends on the uncertainty impacts over the decision procedure.

		Likelihood				
		Rare	Unlikely	Possible	Likely	Certain
Consequence	Critical					
	Major					
	Moderate					
	Minor					
	Insignificant					

How can we Represent Uncertainty?

Using qualitative scales

- uncertainty should be expressed as a separate attribute
- E.g., as a separate natural language expression for each measurement according to an ordinal scale.

Table 13.1 Consequence of incidents with uncertainty estimates

Incident	Consequence	Uncertainty
Information leakage	Low	Some
Breakdown of server	High	No
Identity theft	High	Considerable
Spyware installed	Medium	Some

Reducing Uncertainty

We may use different assessment methods to reduce uncertainty using data already acquired

- Fuzzy logic
- Iterating data collection
- Comparative Analysis
- Testing the risk model against historical data or by conducting various surveys across larger groups of stakeholders.

High-consequence Risk with Low Likelihood

A **black swan** is an incident that is extremely rare and unexpected, but has very significant consequences

Black swans are not likely to be discovered by risk assessment

- developing good contingency plans is the best approach to cope with black swans
- risk assessment does not make contingency planning (i.e., the act of preparing and planning for major incidents and disasters) obsolete

High-consequence Risk with Low Likelihood

A *gray swan* is an incident which has far-reaching consequences, but, unlike a black swan, can be anticipated to a certain degree

WARNING: gray swans may also easily be overlooked

- they are not present in the documentation that we (as risk assessors) consider as input
- we are not interacting with the right group of stakeholders
- we are not able to extract the required information
- by definition, there is knowledge of all relevant gray swans within the context of the target of assessment, if not explicitly written down in some document then at least implicitly within the mind of a stakeholder or deducible from the available data

Communicating Gray Swans

It is fundamental to define an effective process to convey the good message to managers

- Using probability is not recommended
- When using quantitative scale, always use a reference
- if there is considerable uncertainty then it must be communicated to relevant decision makers

Dealing with Gray Swans

We are in the treatment phase trying to aid the decision makers in making the right decision regarding a gray swan.

Cost of Treatment

Low

Treat the Gray Swans



High



Likelihood



Consequence