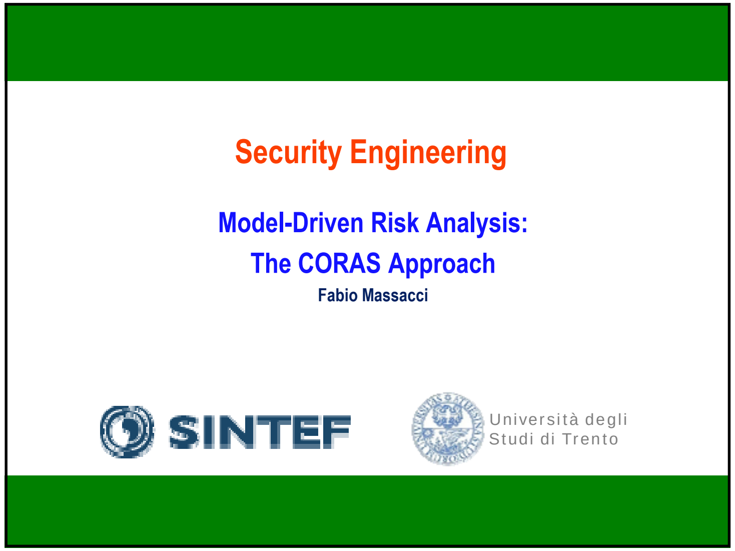


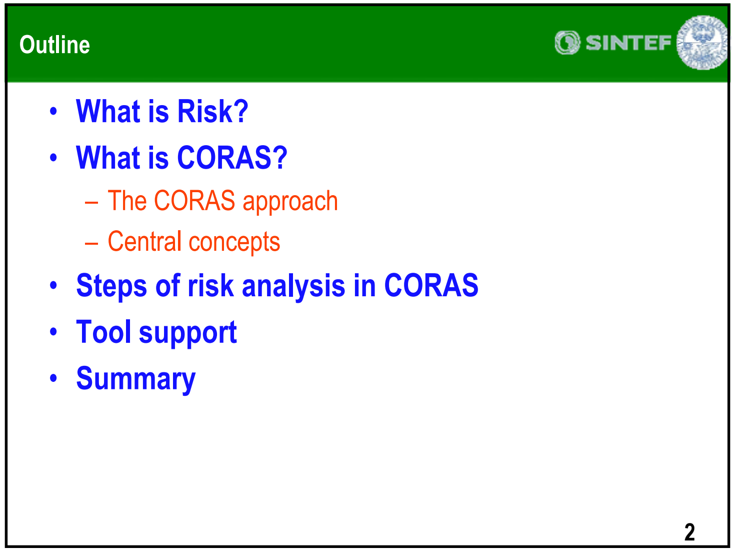
# Security Engineering

## Model-Driven Risk Analysis: The CORAS Approach

Fabio Massacci

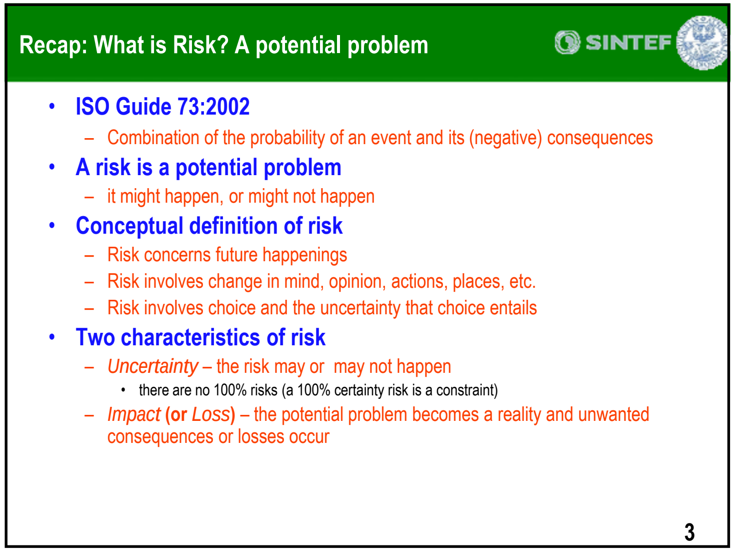
SINTEF

Università degli Studi di Trento



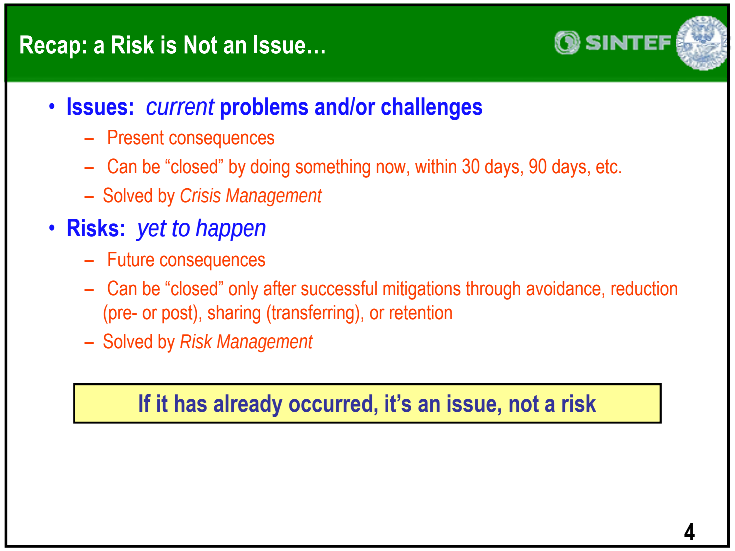
## Outline

- What is Risk?
- What is CORAS?
  - The CORAS approach
  - Central concepts
- Steps of risk analysis in CORAS
- Tool support
- Summary



## Recap: What is Risk? A potential problem

- ISO Guide 73:2002
  - Combination of the probability of an event and its (negative) consequences
- A risk is a potential problem
  - it might happen, or might not happen
- Conceptual definition of risk
  - Risk concerns future happenings
  - Risk involves change in mind, opinion, actions, places, etc.
  - Risk involves choice and the uncertainty that choice entails
- Two characteristics of risk
  - *Uncertainty* – the risk may or may not happen
    - there are no 100% risks (a 100% certainty risk is a constraint)
  - *Impact* (or *Loss*) – the potential problem becomes a reality and unwanted consequences or losses occur



## Recap: a Risk is Not an Issue…

- Issues: *current* problems and/or challenges
  - Present consequences
  - Can be "closed" by doing something now, within 30 days, 90 days, etc.
  - Solved by *Crisis Management*
- Risks: *yet to happen*
  - Future consequences
  - Can be "closed" only after successful mitigations through avoidance, reduction (pre- or post), sharing (transferring), or retention
  - Solved by *Risk Management*

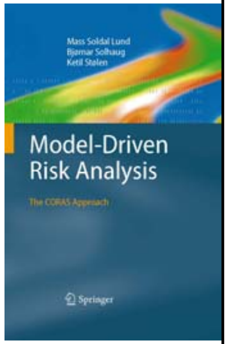
**If it has already occurred, it's an issue, not a risk**

## What is Risk Analysis?

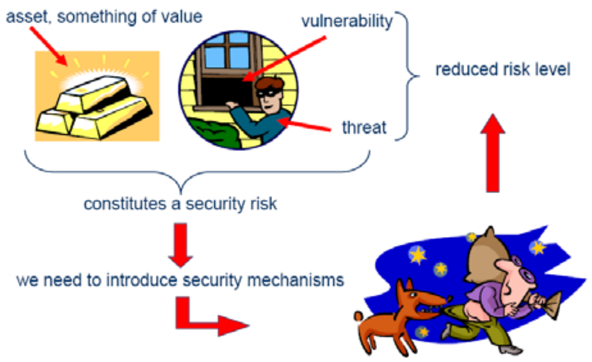
- Risk analysis tries to answer
  - What can go wrong?
  - How likely is it to happen?
  - What the consequences of going wrong?
  - What opportunities I lose if decide to mitigate the risk?
- [T. Bedford and R. Cooke, Probabilistic Risk Analysis: Foundations and Methods, 2001]

## What is CORAS?

- The CORAS approach:
  - A language for risk modeling
  - A tool to support the risk analysis process
  - A method for risk analysis
    - A stepwise, structured and systematic process
    - Asset-driven
    - Concrete tasks with practical guidelines
    - Model-driven
      - Models as basis for and input to analysis tasks
      - Models for documentation of results
- Based on internationally established standards (*ISO 31000)*
- Book: http://www.springer.com/computer/swe/book/978-3-642-12322-1

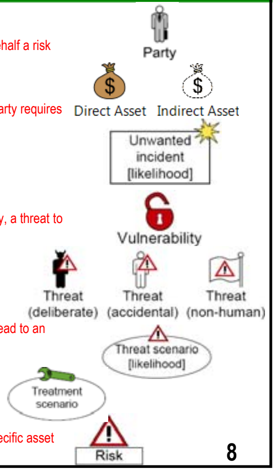


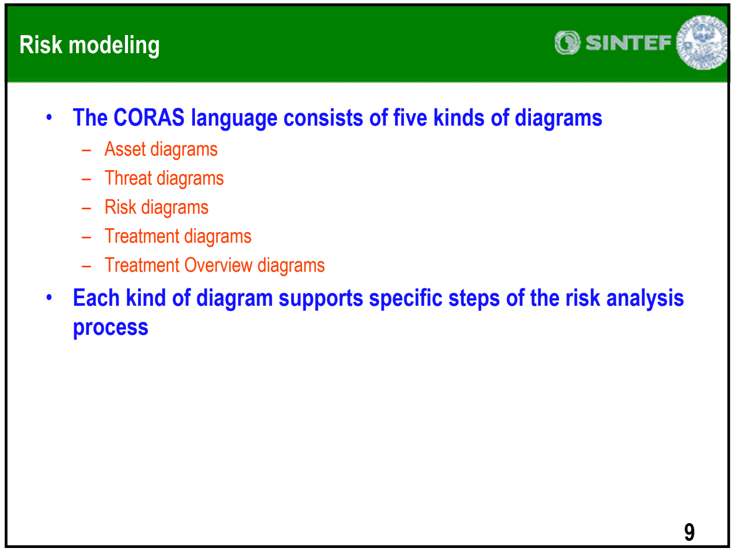
## Terms


asset, something of value
vulnerability
threat
reduced risk level
constitutes a security risk
we need to introduce security mechanisms

## CORAS Modeling Concepts

- Party:
  - An organization, company, person, group or other body on whose behalf a risk analysis is conducted
- Asset:
  - Something to which a party assigns value and hence for which the party requires protection
- Unwanted incident:
  - An event that harms or reduces the value of an asset
- Vulnerability:
  - A weakness, flaw or deficiency that opens for, or may be exploited by, a threat to cause harm to or reduce the value of an asset
- Threat:
  - A potential cause of an unwanted incident
- Threat scenario:
  - A chain or series of events that is initiated by a threat and that may lead to an unwanted incident
- Treatment (Treatment Scenario):
  - An appropriate measure to reduce risk level
- Risk:
  - The likelihood of an unwanted incident and its consequence for a specific asset

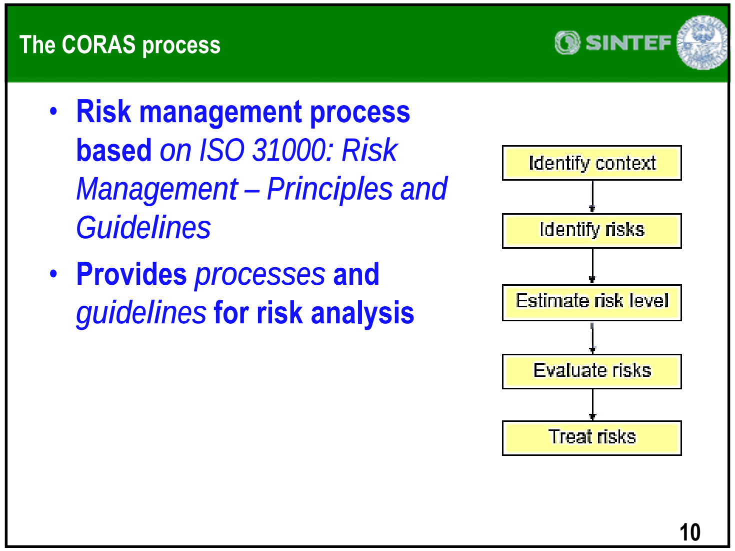




## Risk modeling

SINTEF

- The CORAS language consists of five kinds of diagrams
  - Asset diagrams
  - Threat diagrams
  - Risk diagrams
  - Treatment diagrams
  - Treatment Overview diagrams
- Each kind of diagram supports specific steps of the risk analysis process

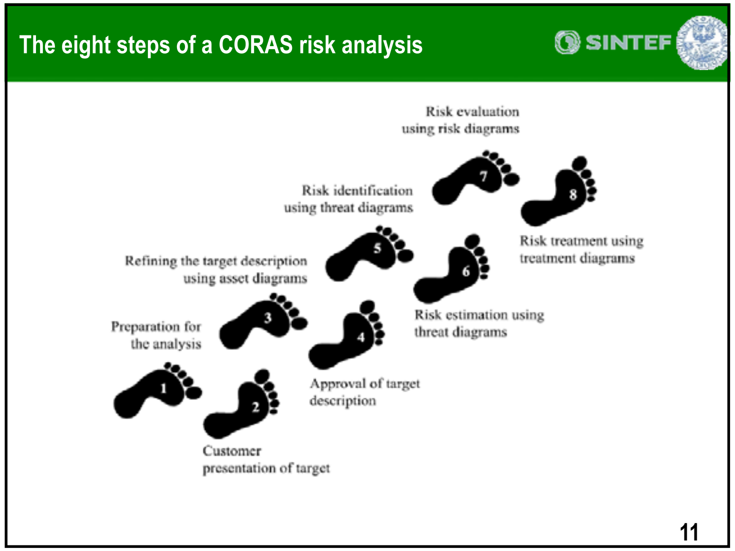


## The CORAS process

SINTEF

- **Risk management process based** *on ISO 31000: Risk Management – Principles and Guidelines*
- **Provides** *processes* **and** *guidelines* **for risk analysis**

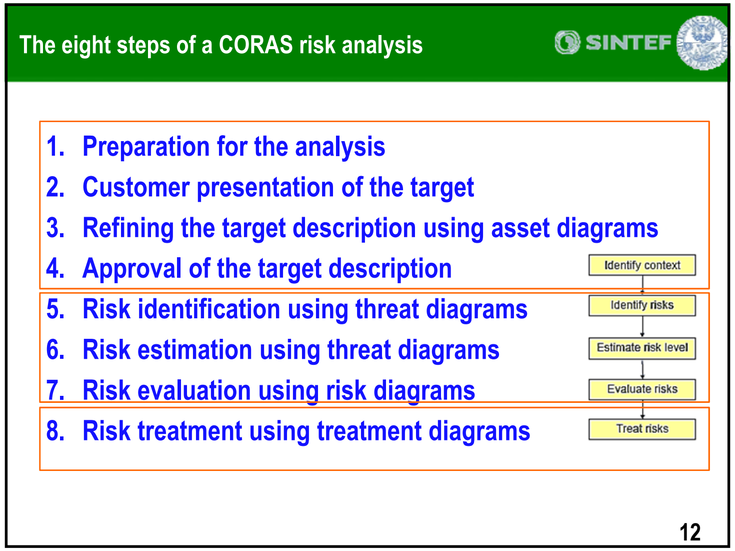
Identify context → Identify risks → Estimate risk level → Evaluate risks → Treat risks



## The eight steps of a CORAS risk analysis

SINTEF

1
Preparation for the analysis
2
Customer presentation of target
3
Refining the target description using asset diagrams
4
Approval of target description
5
Risk identification using threat diagrams
6
Risk estimation using threat diagrams
7
Risk evaluation using risk diagrams
8
Risk treatment using treatment diagrams



## The eight steps of a CORAS risk analysis

SINTEF

1. Preparation for the analysis
2. Customer presentation of the target
3. Refining the target description using asset diagrams
4. Approval of the target description
5. Risk identification using threat diagrams
6. Risk estimation using threat diagrams
7. Risk evaluation using risk diagrams
8. Risk treatment using treatment diagrams

Identify context → Identify risks → Estimate risk level → Evaluate risks → Treat risks

## Step 1: Preparation for the analysis

- **Objective: do the necessary initial preparations prior to the actual startup of the analysis**
- **Tasks:**
  - Contact the customer for the case study
  - Roughly setting the scope and focus

## Example: Local Bank

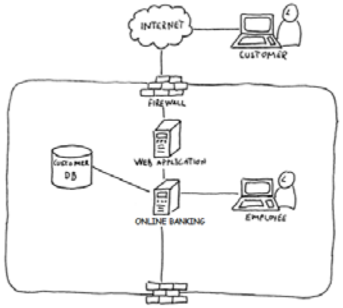
- Local Bank is a private bank. Its business is to offer financial services in the banking domain for customers
- Local Bank has a web application and a online banking system
- Local Bank is using a database to manage the customer data such as: personal information, payment card(s), and so on
- Local Bank has decided it wants to do a risk analysis of the system
- Of particular concern for the management is:
  - The web application for customer
  - The online banking system that connects both the customer database and the web application

## Step 2: Customer presentation of the target

- **Objective: achieve an initial understanding of the target of risk analysis**
- **Tasks:**
  - Customer presentation on the target
  - Target to be understood by risk analysts
  - Set the focus of the analysis
- **Artifact to be produced:**
  - Description of the target:
    - The overall goals of the analysis
    - The target that wishes to have analyzed

## Example: Customer presentation on the target

- **Understand customer's goals and target:**
  - Of particular concern for the management is:
    - the web application that connects to both their customer database and their online banking.

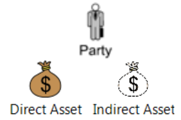


## Step 3: Refining the target description using asset diagrams

- **Objective: ensure a common and more precise understanding of the target analysis, including its scope, focus, and main assets**
- Task:
  - The target is understood by the risk analysts
  - Identify the parties and assets
  - Conduct a high-level analysis:
    - The first threats, vulnerabilities, threat scenarios and unwanted incidents are identified.
- **Artifacts to be produced:**
  - Asset diagram
  - High-level analysis: preliminary list of Unwanted incidents

## Identify asset

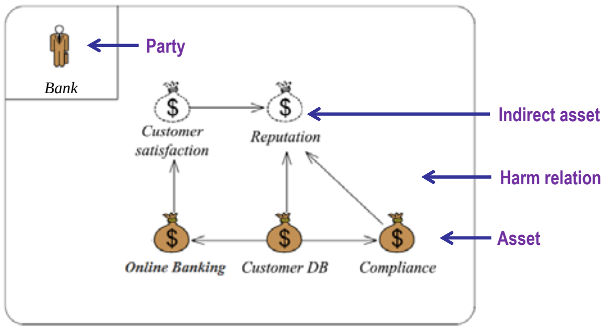
- Identify involving party
  - An organization, company, person, group or other body on whose behalf a risk analysis is conducted
- Identify asset of each party intends to protect
  - Something to which a party assigns value and hence for which the party requires protection
  - The “THINGS” that are valuable
- Notions to be used in Asset Diagram



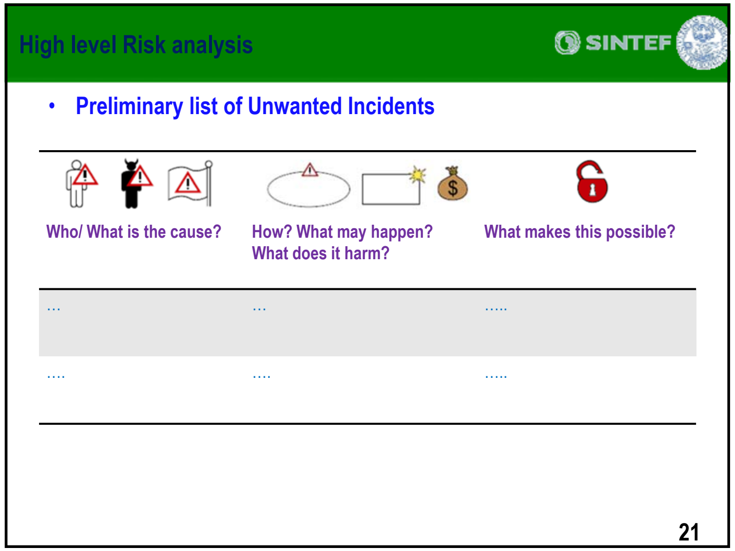
## Example: Identify Party and Asset

- **Party:**
  - Bank company??
- **Asset:**
  - Customer DB
  - Online banking
  - Compliance
  - Company reputation
  - Customer satisfaction

## Example: Asset diagram



- **Relations between assets**
  - Harm in one asset might harm also other assets.

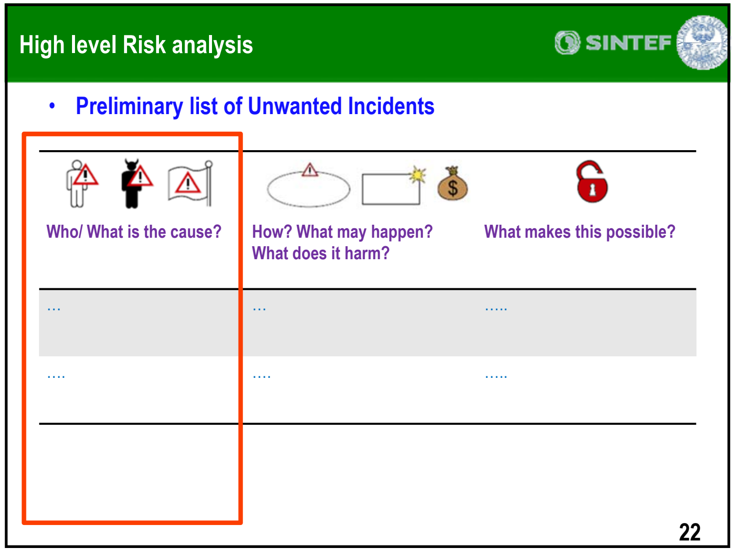


## High level Risk analysis

- Preliminary list of Unwanted Incidents

| Who/ What is the cause? | How? What may happen?<br>What does it harm? | What makes this possible? |
|---|---|---|
| … | … | ….. |
| …. | …. | ….. |

21

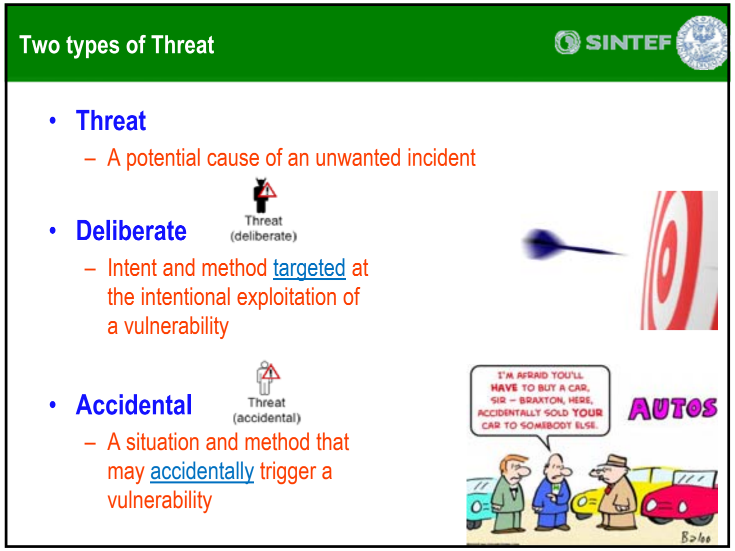


## High level Risk analysis

- Preliminary list of Unwanted Incidents

| Who/ What is the cause? | How? What may happen?<br>What does it harm? | What makes this possible? |
|---|---|---|
| … | … | ….. |
| …. | …. | ….. |

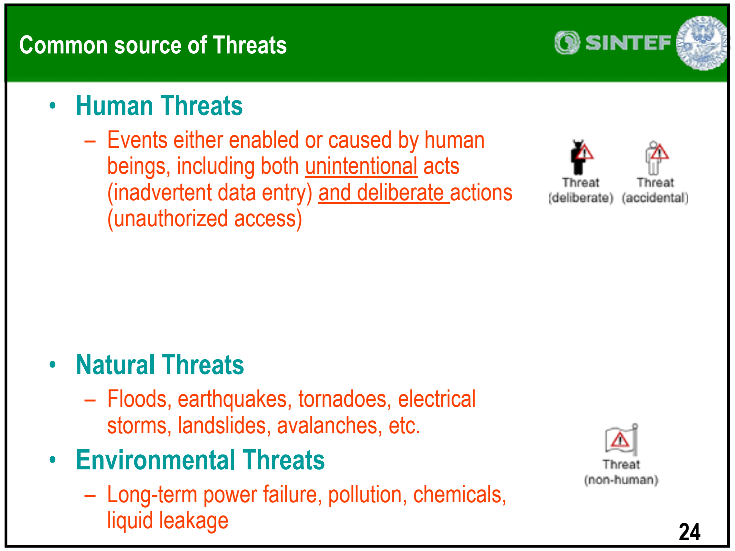
22



## Two types of Threat

- Threat
  - A potential cause of an unwanted incident
- Deliberate (Threat (deliberate))
  - Intent and method targeted at the intentional exploitation of a vulnerability
- Accidental (Threat (accidental))
  - A situation and method that may accidentally trigger a vulnerability

I'M AFRAID YOU'LL HAVE TO BUY A CAR, SIR – BRAXTON, HERE, ACCIDENTALLY SOLD YOUR CAR TO SOMEBODY ELSE.
AUTOS



## Common source of Threats

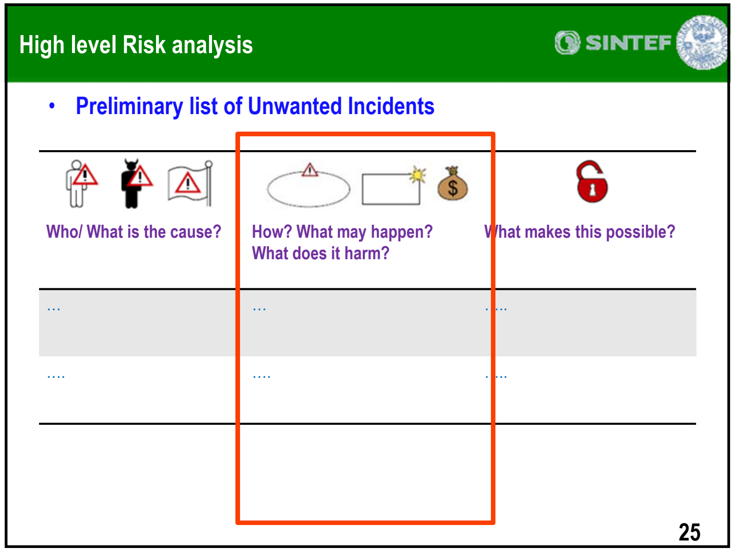
- Human Threats
  - Events either enabled or caused by human beings, including both unintentional acts (inadvertent data entry) and deliberate actions (unauthorized access)

Threat (deliberate) Threat (accidental)

- Natural Threats
  - Floods, earthquakes, tornadoes, electrical storms, landslides, avalanches, etc.
- Environmental Threats
  - Long-term power failure, pollution, chemicals, liquid leakage

Threat (non-human)

24

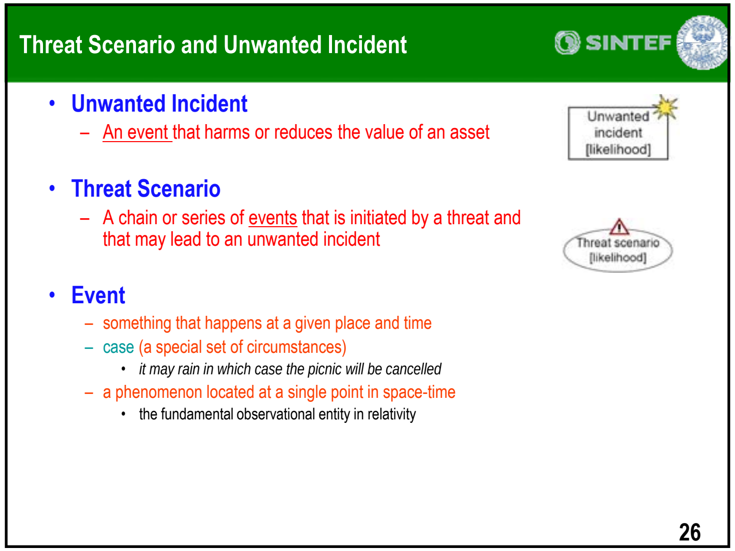


## High level Risk analysis

- **Preliminary list of Unwanted Incidents**

| Who/ What is the cause? | How? What may happen?<br>What does it harm? | What makes this possible? |
|---|---|---|
| … | … | ….. |
| …. | …. | ….. |

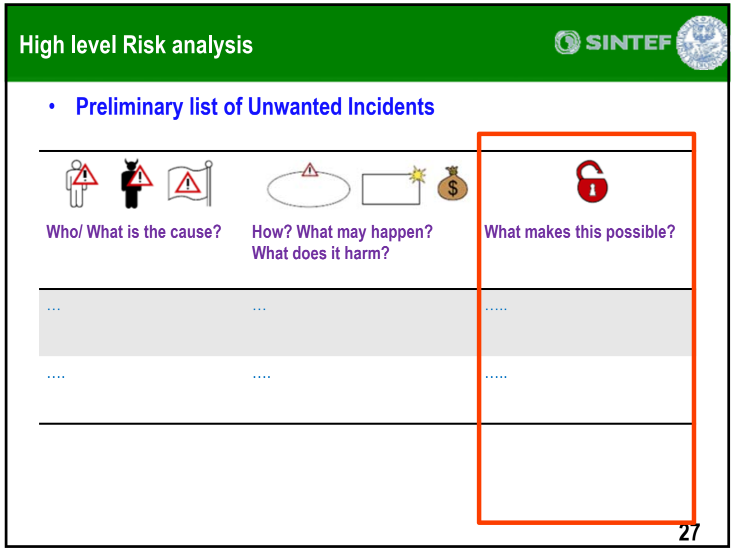
25



## Threat Scenario and Unwanted Incident

- **Unwanted Incident**
  - An event that harms or reduces the value of an asset
- **Threat Scenario**
  - A chain or series of events that is initiated by a threat and that may lead to an unwanted incident
- **Event**
  - something that happens at a given place and time
  - case (a special set of circumstances)
    - *it may rain in which case the picnic will be cancelled*
  - a phenomenon located at a single point in space-time
    - the fundamental observational entity in relativity

26

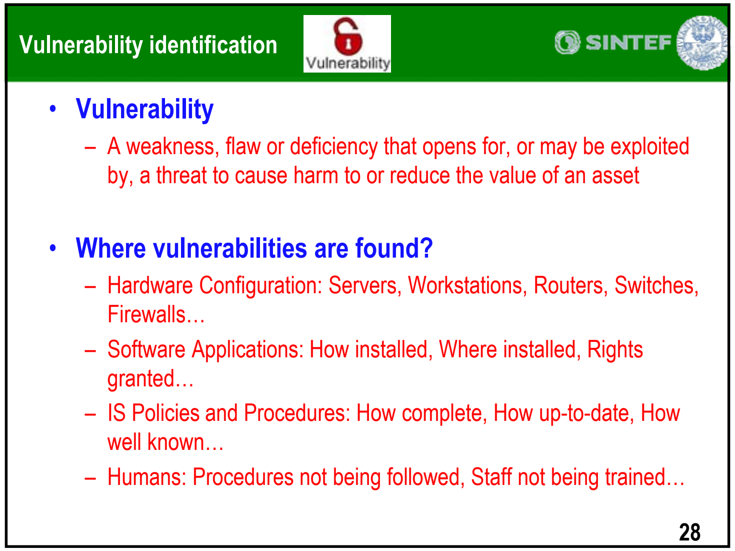


## High level Risk analysis

- **Preliminary list of Unwanted Incidents**

| Who/ What is the cause? | How? What may happen?<br>What does it harm? | What makes this possible? |
|---|---|---|
| … | … | ….. |
| …. | …. | ….. |

27

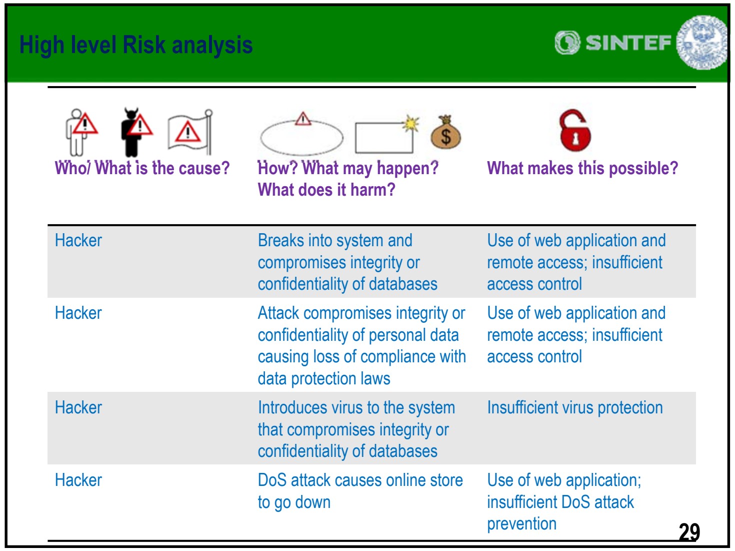


## Vulnerability identification

Vulnerability

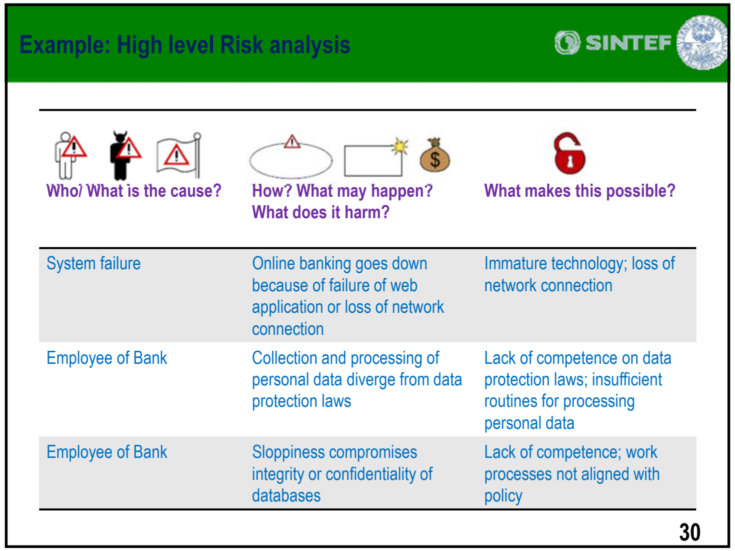
- **Vulnerability**
  - A weakness, flaw or deficiency that opens for, or may be exploited by, a threat to cause harm to or reduce the value of an asset
- **Where vulnerabilities are found?**
  - Hardware Configuration: Servers, Workstations, Routers, Switches, Firewalls…
  - Software Applications: How installed, Where installed, Rights granted…
  - IS Policies and Procedures: How complete, How up-to-date, How well known…
  - Humans: Procedures not being followed, Staff not being trained…

28



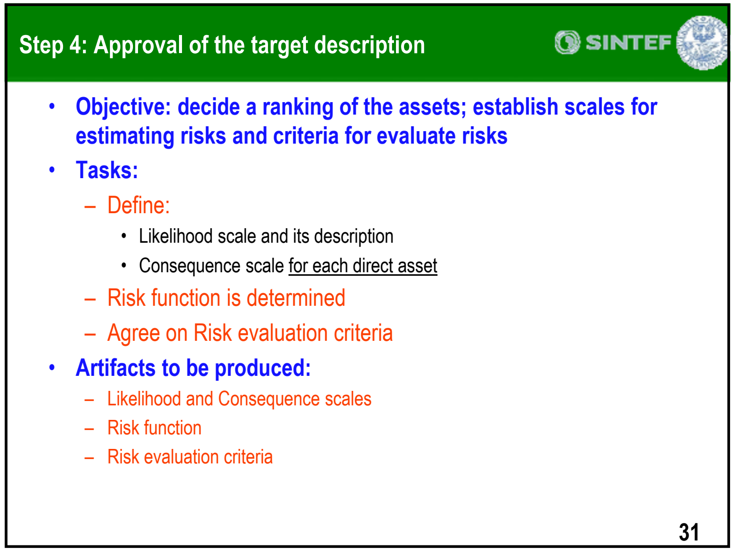
## High level Risk analysis

| Who/ What is the cause? | How? What may happen? What does it harm? | What makes this possible? |
|---|---|---|
| Hacker | Breaks into system and compromises integrity or confidentiality of databases | Use of web application and remote access; insufficient access control |
| Hacker | Attack compromises integrity or confidentiality of personal data causing loss of compliance with data protection laws | Use of web application and remote access; insufficient access control |
| Hacker | Introduces virus to the system that compromises integrity or confidentiality of databases | Insufficient virus protection |
| Hacker | DoS attack causes online store to go down | Use of web application; insufficient DoS attack prevention |



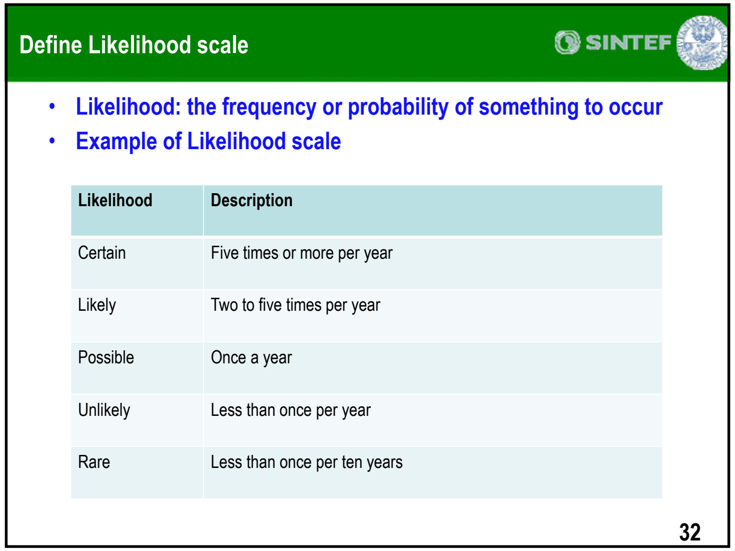
## Example: High level Risk analysis

| Who/ What is the cause? | How? What may happen? What does it harm? | What makes this possible? |
|---|---|---|
| System failure | Online banking goes down because of failure of web application or loss of network connection | Immature technology; loss of network connection |
| Employee of Bank | Collection and processing of personal data diverge from data protection laws | Lack of competence on data protection laws; insufficient routines for processing personal data |
| Employee of Bank | Sloppiness compromises integrity or confidentiality of databases | Lack of competence; work processes not aligned with policy |



## Step 4: Approval of the target description

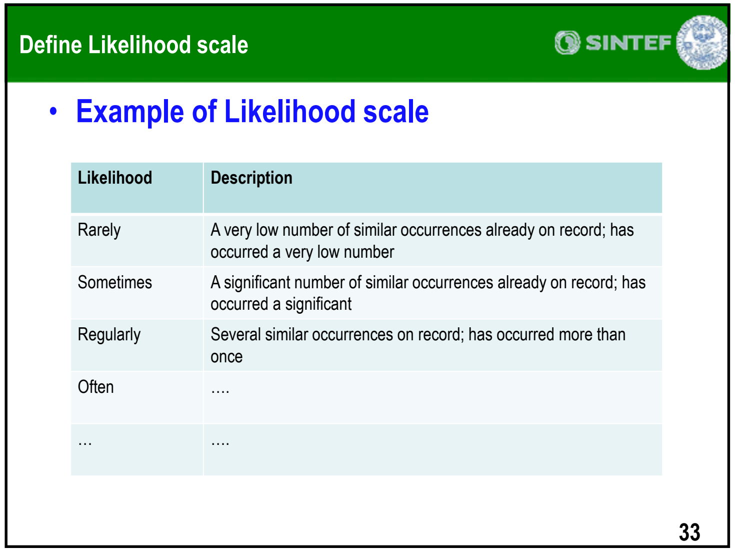
- Objective: decide a ranking of the assets; establish scales for estimating risks and criteria for evaluate risks
- Tasks:
  - Define:
    - Likelihood scale and its description
    - Consequence scale for each direct asset
  - Risk function is determined
  - Agree on Risk evaluation criteria
- Artifacts to be produced:
  - Likelihood and Consequence scales
  - Risk function
  - Risk evaluation criteria



## Define Likelihood scale

- Likelihood: the frequency or probability of something to occur
- Example of Likelihood scale

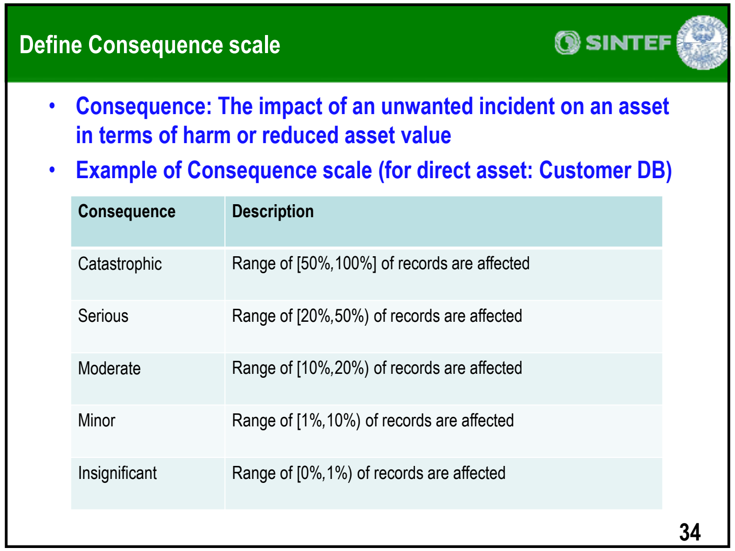
| Likelihood | Description |
|---|---|
| Certain | Five times or more per year |
| Likely | Two to five times per year |
| Possible | Once a year |
| Unlikely | Less than once per year |
| Rare | Less than once per ten years |



## Define Likelihood scale

- **Example of Likelihood scale**

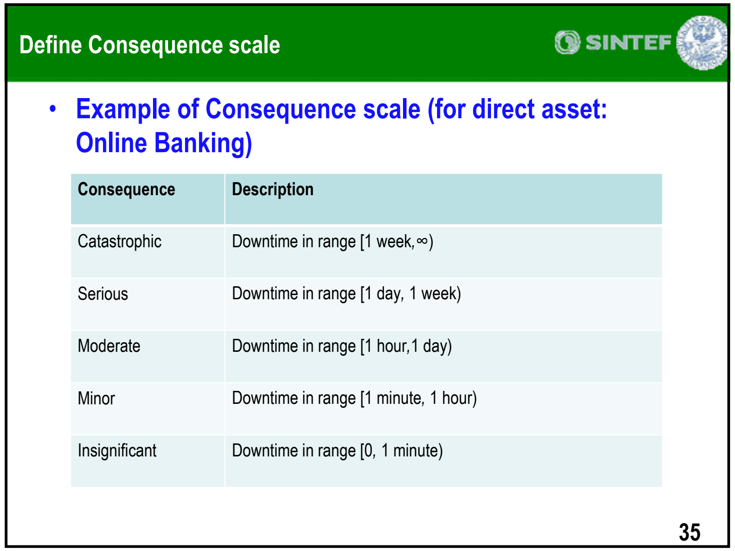
| Likelihood | Description |
|---|---|
| Rarely | A very low number of similar occurrences already on record; has occurred a very low number |
| Sometimes | A significant number of similar occurrences already on record; has occurred a significant |
| Regularly | Several similar occurrences on record; has occurred more than once |
| Often | …. |
| … | …. |



## Define Consequence scale

- **Consequence: The impact of an unwanted incident on an asset in terms of harm or reduced asset value**
- **Example of Consequence scale (for direct asset: Customer DB)**

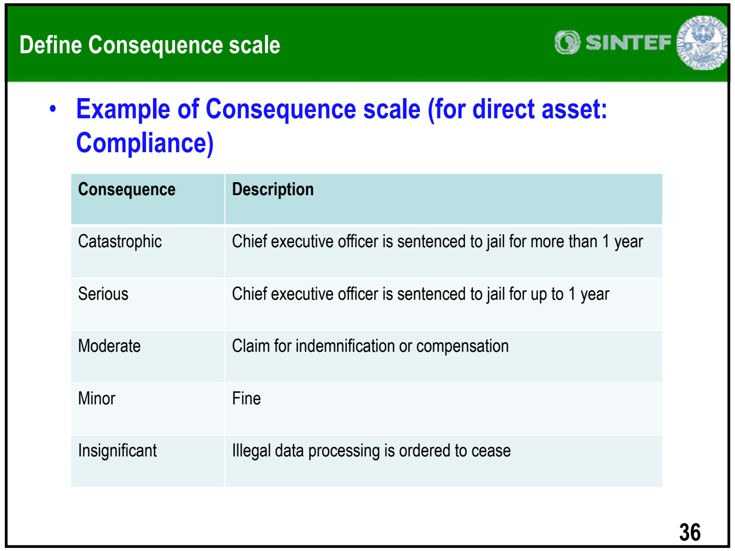
| Consequence | Description |
|---|---|
| Catastrophic | Range of [50%,100%] of records are affected |
| Serious | Range of [20%,50%) of records are affected |
| Moderate | Range of [10%,20%) of records are affected |
| Minor | Range of [1%,10%) of records are affected |
| Insignificant | Range of [0%,1%) of records are affected |



## Define Consequence scale

- **Example of Consequence scale (for direct asset: Online Banking)**

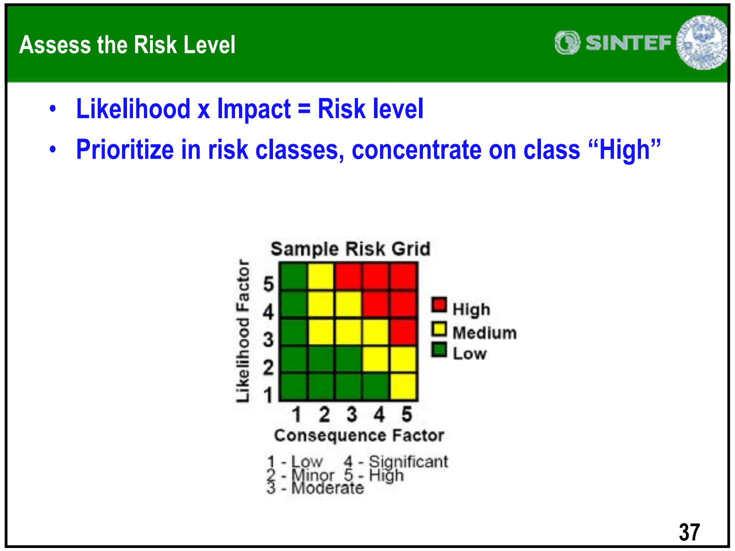
| Consequence | Description |
|---|---|
| Catastrophic | Downtime in range [1 week,∞) |
| Serious | Downtime in range [1 day, 1 week) |
| Moderate | Downtime in range [1 hour,1 day) |
| Minor | Downtime in range [1 minute, 1 hour) |
| Insignificant | Downtime in range [0, 1 minute) |



## Define Consequence scale

- **Example of Consequence scale (for direct asset: Compliance)**

| Consequence | Description |
|---|---|
| Catastrophic | Chief executive officer is sentenced to jail for more than 1 year |
| Serious | Chief executive officer is sentenced to jail for up to 1 year |
| Moderate | Claim for indemnification or compensation |
| Minor | Fine |
| Insignificant | Illegal data processing is ordered to cease |



## Assess the Risk Level

- Likelihood x Impact = Risk level
- Prioritize in risk classes, concentrate on class "High"

Sample Risk Grid

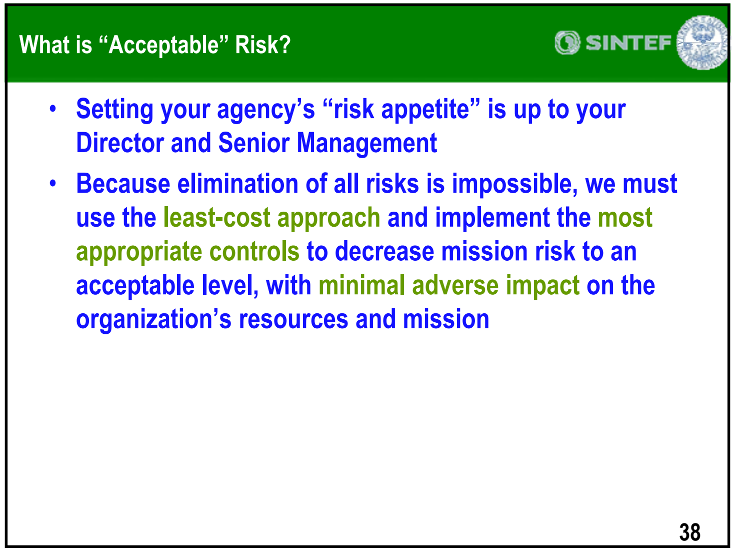
| Likelihood Factor | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|
| 5 | 🟩 | 🟨 | 🟥 | 🟥 | 🟥 |
| 4 | 🟩 | 🟨 | 🟨 | 🟥 | 🟥 |
| 3 | 🟩 | 🟨 | 🟨 | 🟨 | 🟥 |
| 2 | 🟩 | 🟩 | 🟩 | 🟨 | 🟨 |
| 1 | 🟩 | 🟩 | 🟩 | 🟩 | 🟨 |

Consequence Factor

🟥 High
🟨 Medium
🟩 Low

1 - Low 4 - Significant
2 - Minor 5 - High
3 - Moderate

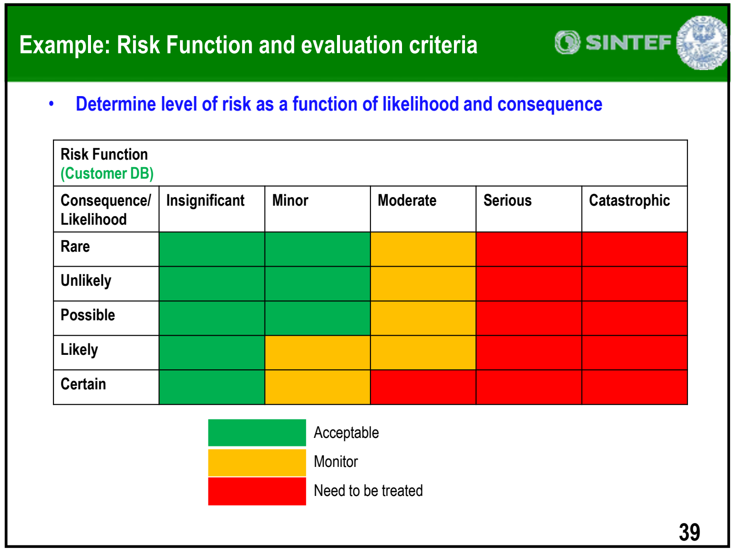
37



## What is "Acceptable" Risk?

- Setting your agency's "risk appetite" is up to your Director and Senior Management
- Because elimination of all risks is impossible, we must use the least-cost approach and implement the most appropriate controls to decrease mission risk to an acceptable level, with minimal adverse impact on the organization's resources and mission

38



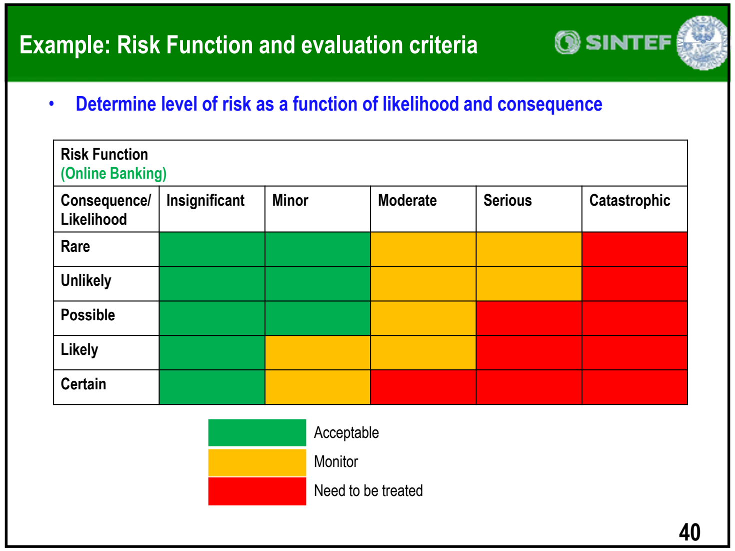
## Example: Risk Function and evaluation criteria

- Determine level of risk as a function of likelihood and consequence

| Risk Function<br>(Customer DB) | | | | | |
|---|---|---|---|---|---|
| Consequence/ Likelihood | Insignificant | Minor | Moderate | Serious | Catastrophic |
| Rare | 🟩 | 🟩 | 🟧 | 🟥 | 🟥 |
| Unlikely | 🟩 | 🟩 | 🟧 | 🟥 | 🟥 |
| Possible | 🟩 | 🟩 | 🟧 | 🟥 | 🟥 |
| Likely | 🟩 | 🟧 | 🟧 | 🟥 | 🟥 |
| Certain | 🟩 | 🟧 | 🟥 | 🟥 | 🟥 |

🟩 Acceptable
🟧 Monitor
🟥 Need to be treated

39



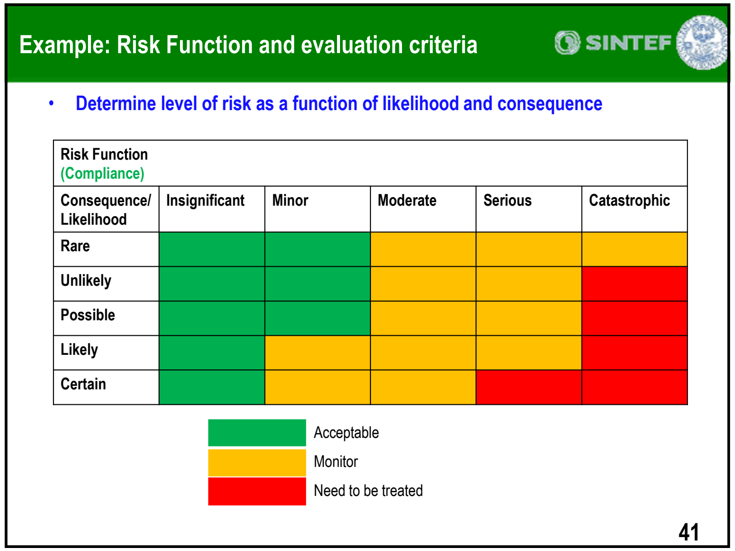
## Example: Risk Function and evaluation criteria

- Determine level of risk as a function of likelihood and consequence

| Risk Function<br>(Online Banking) | | | | | |
|---|---|---|---|---|---|
| Consequence/ Likelihood | Insignificant | Minor | Moderate | Serious | Catastrophic |
| Rare | 🟩 | 🟩 | 🟧 | 🟧 | 🟥 |
| Unlikely | 🟩 | 🟩 | 🟧 | 🟧 | 🟥 |
| Possible | 🟩 | 🟩 | 🟧 | 🟥 | 🟥 |
| Likely | 🟩 | 🟧 | 🟧 | 🟥 | 🟥 |
| Certain | 🟩 | 🟧 | 🟥 | 🟥 | 🟥 |

🟩 Acceptable
🟧 Monitor
🟥 Need to be treated

40

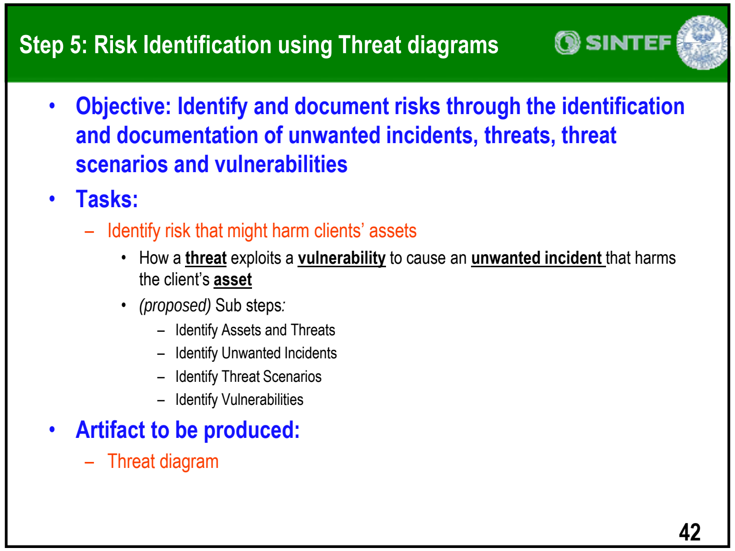


## Example: Risk Function and evaluation criteria

- Determine level of risk as a function of likelihood and consequence

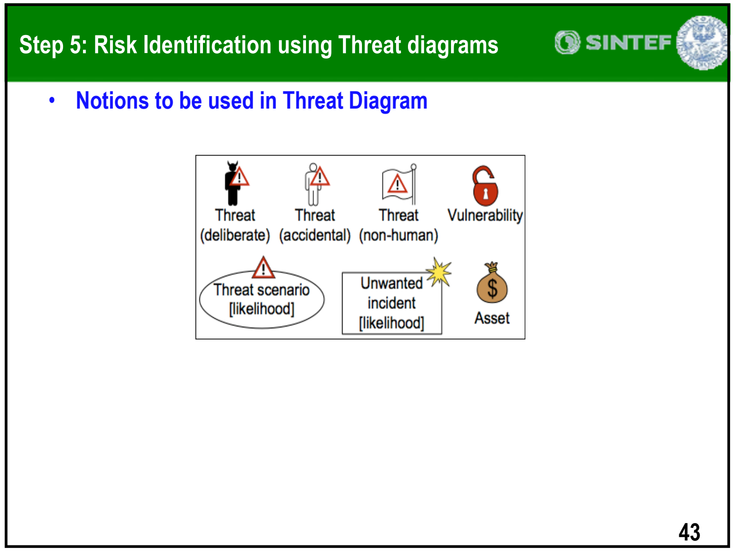
| Risk Function (Compliance) | | | | | |
|---|---|---|---|---|---|
| Consequence/ Likelihood | Insignificant | Minor | Moderate | Serious | Catastrophic |
| Rare | 🟩 | 🟩 | 🟨 | 🟨 | 🟨 |
| Unlikely | 🟩 | 🟩 | 🟨 | 🟨 | 🟥 |
| Possible | 🟩 | 🟩 | 🟨 | 🟨 | 🟥 |
| Likely | 🟩 | 🟨 | 🟨 | 🟨 | 🟥 |
| Certain | 🟩 | 🟨 | 🟨 | 🟥 | 🟥 |

🟩 Acceptable
🟨 Monitor
🟥 Need to be treated



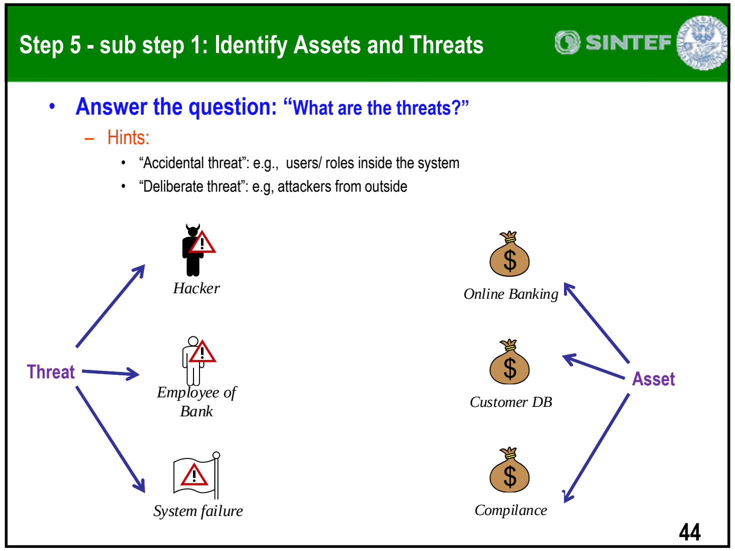
## Step 5: Risk Identification using Threat diagrams

- Objective: Identify and document risks through the identification and documentation of unwanted incidents, threats, threat scenarios and vulnerabilities
- Tasks:
  - Identify risk that might harm clients' assets
    - How a **threat** exploits a **vulnerability** to cause an **unwanted incident** that harms the client's **asset**
    - *(proposed)* Sub steps*:*
      - Identify Assets and Threats
      - Identify Unwanted Incidents
      - Identify Threat Scenarios
      - Identify Vulnerabilities
- Artifact to be produced:
  - Threat diagram



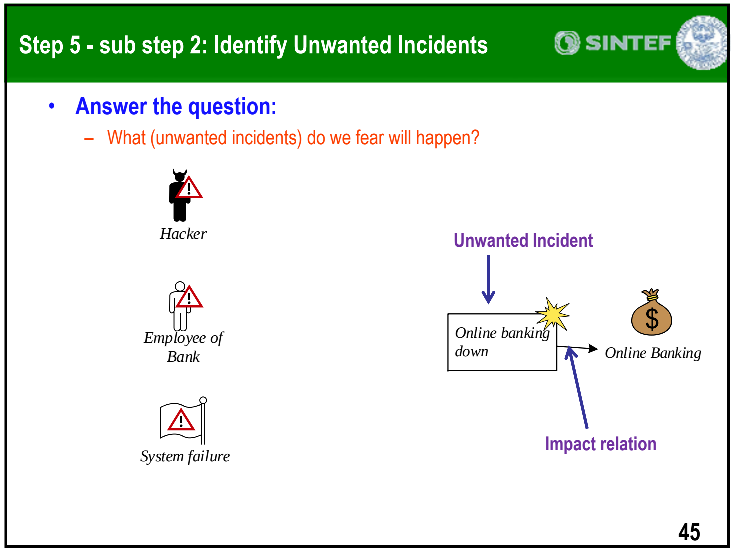
## Step 5: Risk Identification using Threat diagrams

- Notions to be used in Threat Diagram



## Step 5 - sub step 1: Identify Assets and Threats

- Answer the question: "What are the threats?"
  - Hints:
    - "Accidental threat": e.g., users/ roles inside the system
    - "Deliberate threat": e.g, attackers from outside



## Step 5 - sub step 2: Identify Unwanted Incidents

- **Answer the question:**
  - What (unwanted incidents) do we fear will happen?

Hacker

Employee of Bank

System failure

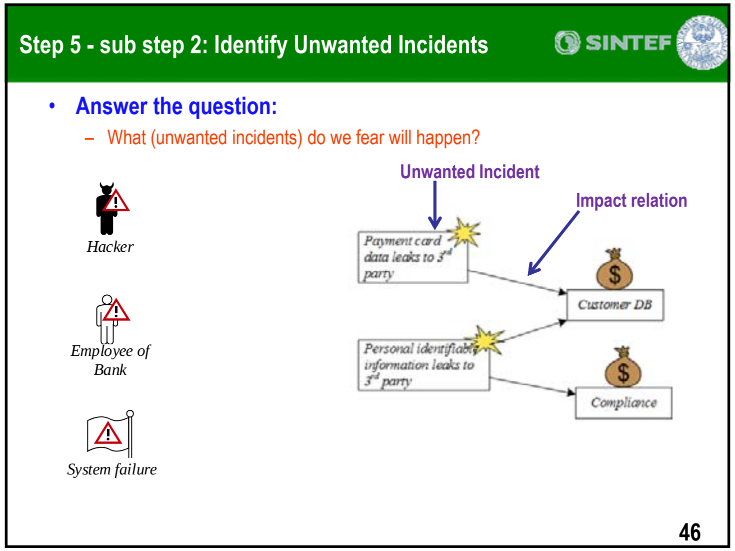
Unwanted Incident

Online banking down

Online Banking

Impact relation

45



## Step 5 - sub step 2: Identify Unwanted Incidents

- **Answer the question:**
  - What (unwanted incidents) do we fear will happen?

Unwanted Incident

Impact relation

Hacker

Employee of Bank

System failure

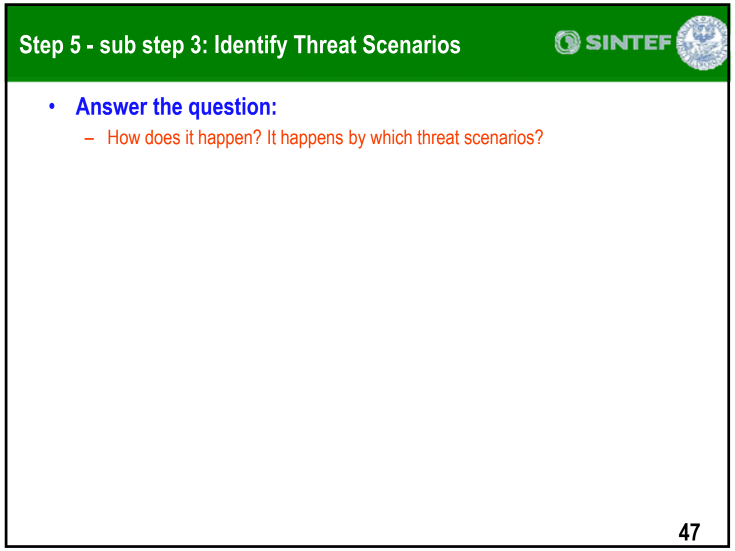
Payment card data leaks to 3rd party

Customer DB

Personal identifiable information leaks to 3rd party

Compliance

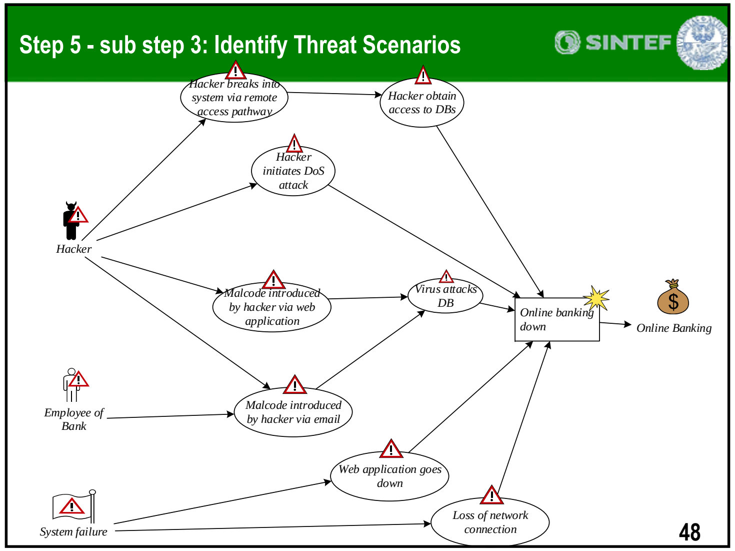
46



## Step 5 - sub step 3: Identify Threat Scenarios

- **Answer the question:**
  - How does it happen? It happens by which threat scenarios?

47



## Step 5 - sub step 3: Identify Threat Scenarios

Hacker breaks into system via remote access pathway

Hacker obtain access to DBs

Hacker initiates DoS attack

Hacker

Malcode introduced by hacker via web application

Virus attacks DB

Online banking down

Online Banking

Employee of Bank

Malcode introduced by hacker via email

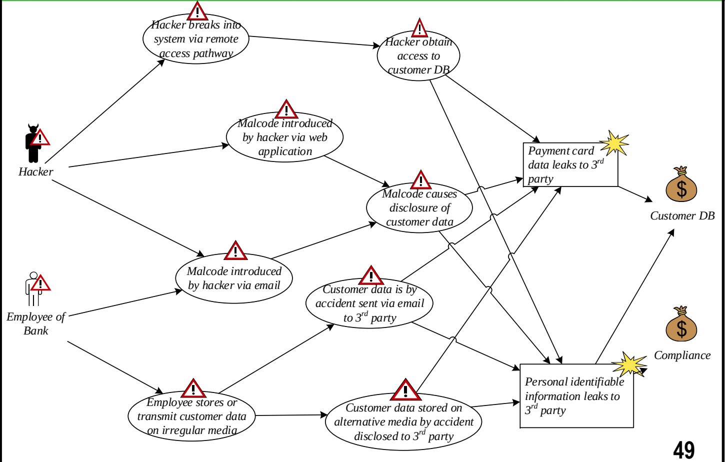
Web application goes down

System failure

Loss of network connection

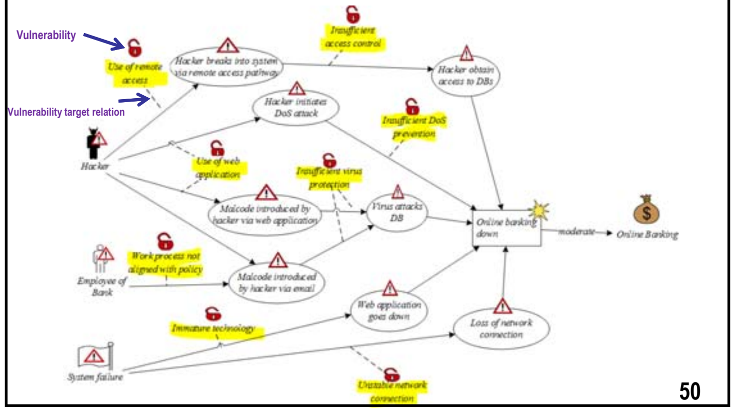
48

## Step 5 - sub step 3: Identify Threat Scenarios

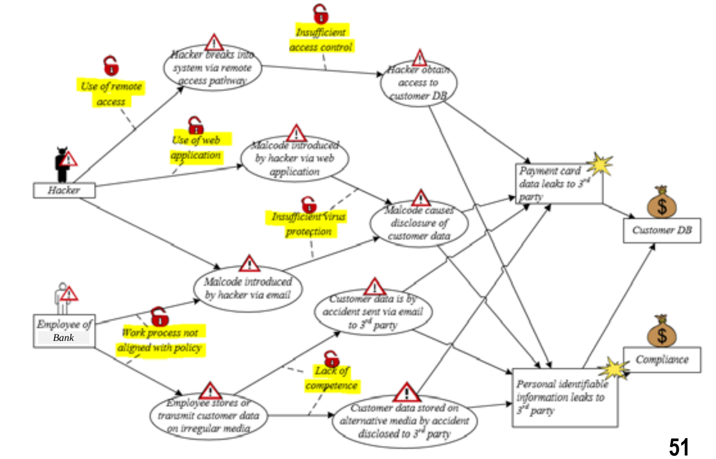

Hacker breaks into system via remote access pathway
Hacker obtain access to customer DB
Malcode introduced by hacker via web application
Hacker
Payment card data leaks to 3rd party
Customer DB
Malcode causes disclosure of customer data
Malcode introduced by hacker via email
Customer data is by accident sent via email to 3rd party
Employee of Bank
Compliance
Personal identifiable information leaks to 3rd party
Employee stores or transmit customer data on irregular media
Customer data stored on alternative media by accident disclosed to 3rd party

## Step 5 - sub step 4: Identify Vulnerabilities

- **Answer the question:**
  - Which vulnerabilities make this possible?

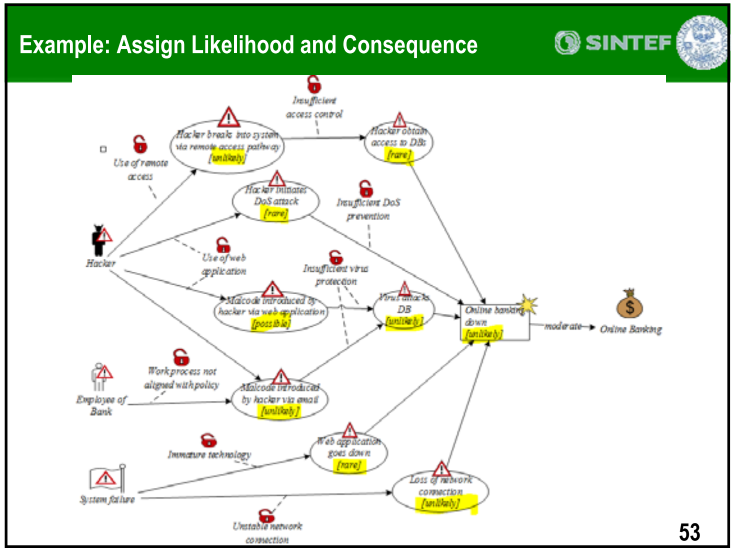

Vulnerability
Vulnerability target relation
Use of remote access
Hacker breaks into system via remote access pathway
Insufficient access control
Hacker obtain access to DBs
Hacker initiates DoS attack
Insufficient DoS prevention
Hacker
Use of web application
Insufficient virus protection
Malcode introduced by hacker via web application
Virus attacks DB
Online banking down
moderate
Online Banking
Employee of Bank
Work process not aligned with policy
Malcode introduced by hacker via email
Web application goes down
Immature technology
Loss of network connection
System failure
Unstable network connection

## Step 5 - sub step 4: Identify Vulnerabilities


Insufficient access control
Use of remote access
Hacker breaks into system via remote access pathway
Hacker obtain access to customer DB
Use of web application
Malcode introduced by hacker via web application
Hacker
Payment card data leaks to 3rd party
Insufficient virus protection
Malcode causes disclosure of customer data
Customer DB
Malcode introduced by hacker via email
Customer data is by accident sent via email to 3rd party
Employee of Bank
Work process not aligned with policy
Compliance
Lack of competence
Personal identifiable information leaks to 3rd party
Employee stores or transmit customer data on irregular media
Customer data stored on alternative media by accident disclosed to 3rd party

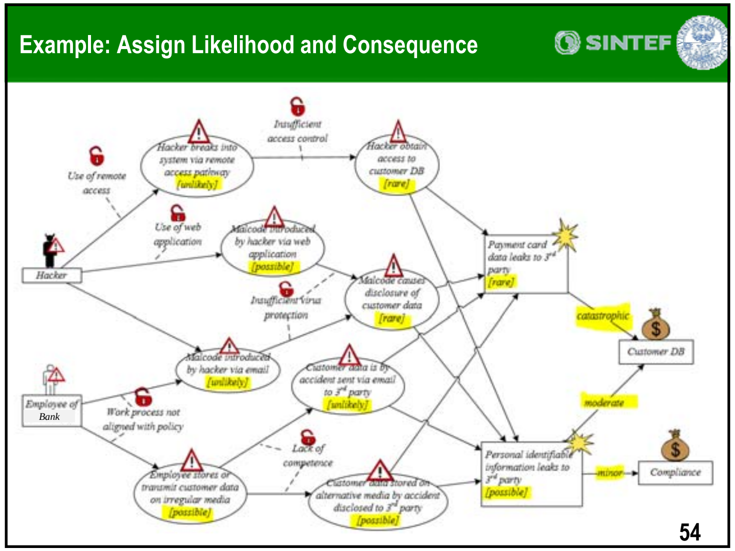
## Step 6: Risk estimation using threat diagrams

- **Objective: determine risk level of the identified risks**
- **Tasks: base on likelihood and consequence scale approved in Step 4**
  - Assign likelihood estimated for each Threat Scenario
  - Assign likelihood estimated for each Unwanted Incidents
  - Assign consequence caused by each Unwanted Incidents on each Asset (the consequence is denoted on “impact” relation
- **Artifacts to be produced:**
  - Completed Threat diagrams with likelihood and consequences assigned



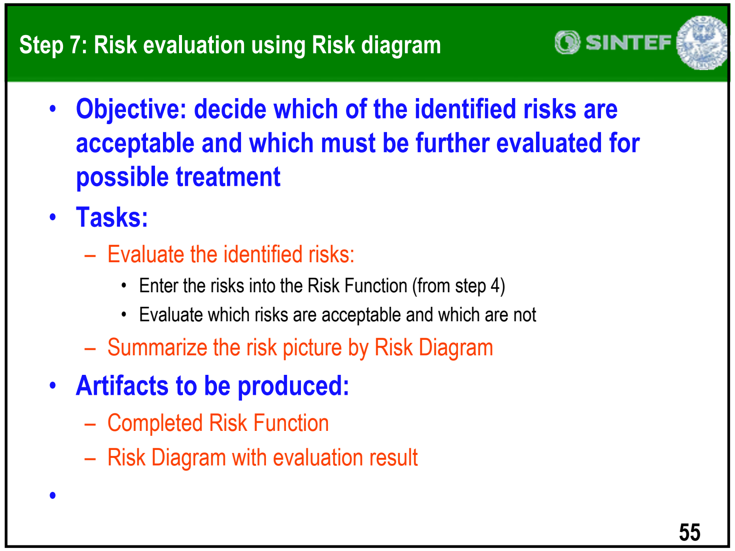
## Example: Assign Likelihood and Consequence

SINTEF
Insufficient access control
Hacker breaks into system via remote access pathway [unlikely]
Hacker obtain access to DBs [rare]
Use of remote access
Hacker initiates DoS attack [rare]
Insufficient DoS prevention
Hacker
Use of web application
Insufficient virus protection
Malcode introduced by hacker via web application [possible]
Virus attacks DB [unlikely]
Online banking down [unlikely]
moderate
Online Banking
Employee of Bank
Work process not aligned with policy
Malcode introduced by hacker via email [unlikely]
Immature technology
Web application goes down [rare]
System failure
Loss of network connection [unlikely]
Unstable network connection



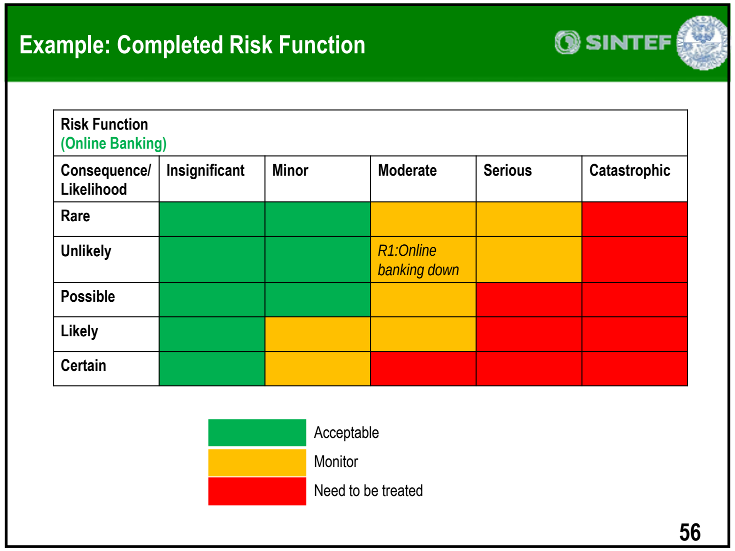
## Example: Assign Likelihood and Consequence

SINTEF
Insufficient access control
Use of remote access
Hacker breaks into system via remote access pathway [unlikely]
Hacker obtain access to customer DB [rare]
Use of web application
Malcode introduced by hacker via web application [possible]
Hacker
Payment card data leaks to 3rd party [rare]
Insufficient virus protection
Malcode causes disclosure of customer data [rare]
catastrophic
Customer DB
Malcode introduced by hacker via email [unlikely]
Customer data is by accident sent via email to 3rd party [unlikely]
Employee of Bank
Work process not aligned with policy
moderate
Lack of competence
Employee stores or transmit customer data on irregular media [possible]
Customer data stored on alternative media by accident disclosed to 3rd party [possible]
Personal identifiable information leaks to 3rd party [possible]
minor
Compliance



## Step 7: Risk evaluation using Risk diagram

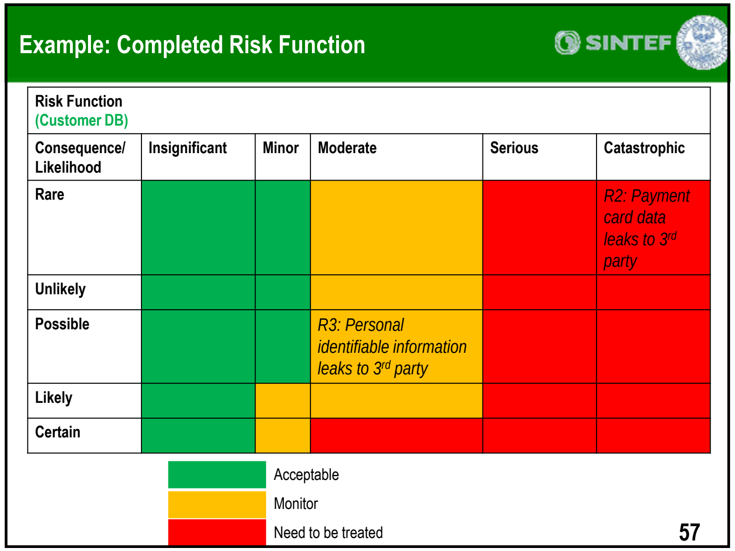
- **Objective: decide which of the identified risks are acceptable and which must be further evaluated for possible treatment**
- **Tasks:**
  - Evaluate the identified risks:
    - Enter the risks into the Risk Function (from step 4)
    - Evaluate which risks are acceptable and which are not
  - Summarize the risk picture by Risk Diagram
- **Artifacts to be produced:**
  - Completed Risk Function
  - Risk Diagram with evaluation result
-



## Example: Completed Risk Function

| Risk Function<br>(Online Banking) | | | | | |
|---|---|---|---|---|---|
| Consequence/ Likelihood | Insignificant | Minor | Moderate | Serious | Catastrophic |
| Rare | 🟩 | 🟩 | 🟨 | 🟨 | 🟥 |
| Unlikely | 🟩 | 🟩 | 🟨 *R1:Online banking down* | 🟨 | 🟥 |
| Possible | 🟩 | 🟩 | 🟨 | 🟥 | 🟥 |
| Likely | 🟩 | 🟨 | 🟨 | 🟥 | 🟥 |
| Certain | 🟩 | 🟨 | 🟥 | 🟥 | 🟥 |

🟩 Acceptable
🟨 Monitor
🟥 Need to be treated



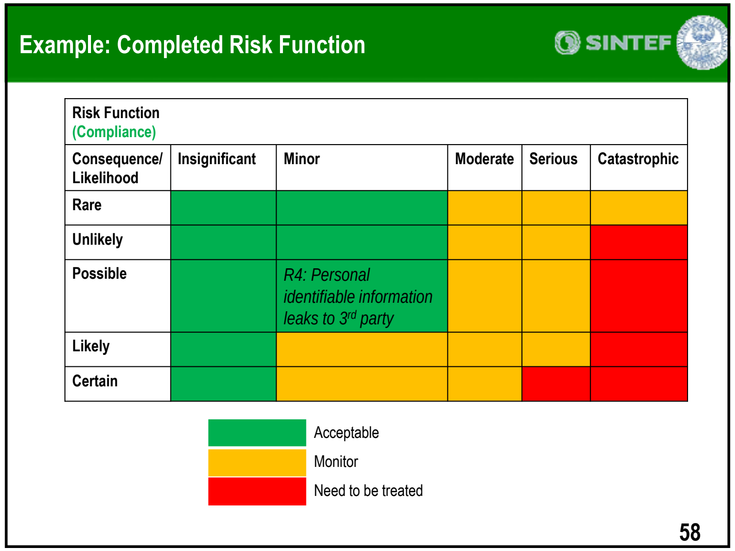
## Example: Completed Risk Function

| Risk Function (Customer DB) | | | | | |
|---|---|---|---|---|---|
| Consequence/ Likelihood | Insignificant | Minor | Moderate | Serious | Catastrophic |
| Rare | 🟩 | 🟩 | 🟨 | 🟥 | 🟥 *R2: Payment card data leaks to 3rd party* |
| Unlikely | 🟩 | 🟩 | 🟨 | 🟥 | 🟥 |
| Possible | 🟩 | 🟩 | 🟨 *R3: Personal identifiable information leaks to 3rd party* | 🟥 | 🟥 |
| Likely | 🟩 | 🟨 | 🟨 | 🟥 | 🟥 |
| Certain | 🟩 | 🟨 | 🟥 | 🟥 | 🟥 |

🟩 Acceptable

🟨 Monitor

🟥 Need to be treated



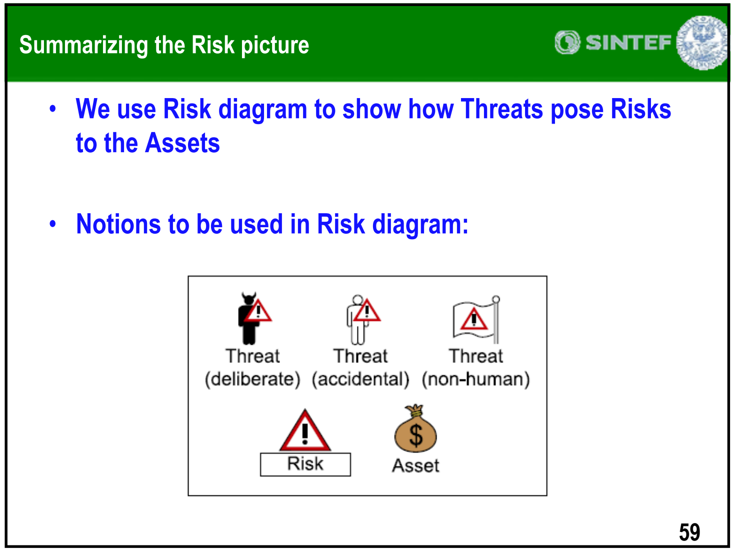
## Example: Completed Risk Function

| Risk Function (Compliance) | | | | | |
|---|---|---|---|---|---|
| Consequence/ Likelihood | Insignificant | Minor | Moderate | Serious | Catastrophic |
| Rare | 🟩 | 🟩 | 🟨 | 🟨 | 🟨 |
| Unlikely | 🟩 | 🟩 | 🟨 | 🟨 | 🟥 |
| Possible | 🟩 | 🟩 *R4: Personal identifiable information leaks to 3rd party* | 🟨 | 🟨 | 🟥 |
| Likely | 🟩 | 🟨 | 🟨 | 🟨 | 🟥 |
| Certain | 🟩 | 🟨 | 🟨 | 🟥 | 🟥 |

🟩 Acceptable

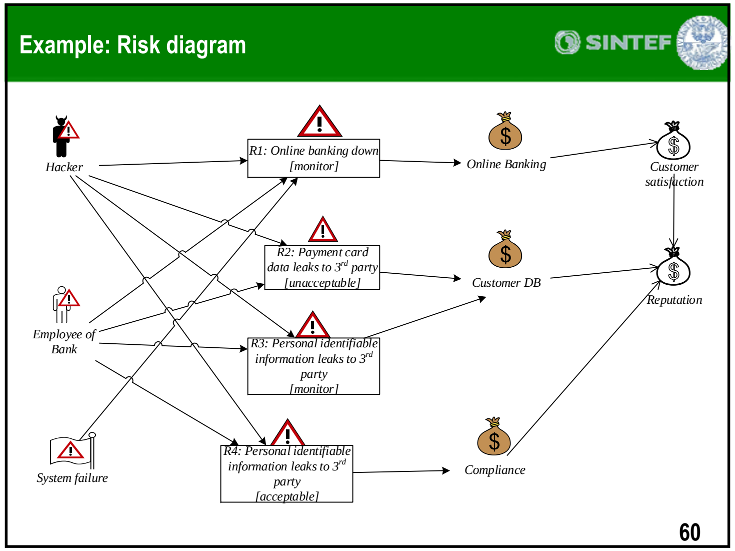
🟨 Monitor

🟥 Need to be treated



## Summarizing the Risk picture

- We use Risk diagram to show how Threats pose Risks to the Assets
- Notions to be used in Risk diagram:



## Example: Risk diagram

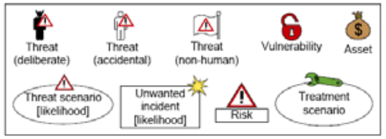
Hacker
Employee of Bank
System failure
R1: Online banking down [monitor]
R2: Payment card data leaks to 3rd party [unacceptable]
R3: Personal identifiable information leaks to 3rd party [monitor]
R4: Personal identifiable information leaks to 3rd party [acceptable]
Online Banking
Customer DB
Compliance
Customer satisfaction
Reputation

## Step 8: Risk treatment using Treatment diagram

- Objective: identify cost effective treatments for the unacceptable risks
- Task:
  - Identify Treatment  Scenario for unacceptable risks:
    - What can we do to reduce the risks to an acceptable (or monitor) level?
  - Create Treatment diagram
  - Summarize by Treatment Overview diagram
  - Evaluate treatment: estimate the cost-benefit of each treatment, and decide which ones to implement
- Artifacts to be produced:
  - Treatment diagram (=Threat diagram with Treatment added)
  - Treatment Overview diagram
  - Treatment evaluation

## Step 8: Risk treatment using treatment diagram

- Notions to be used in Treatment Diagram

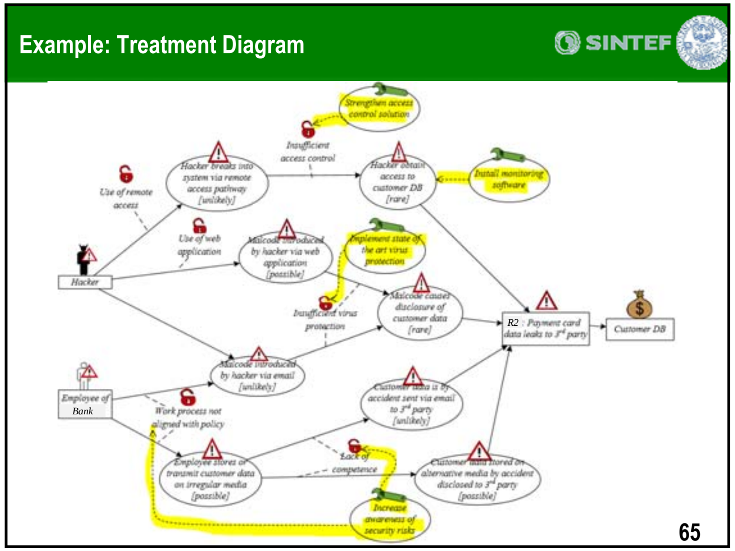


## Identify Treatment

- Start with most severe risks
- List possible actions to reduce likelihood and/or loss
  - What could be done?
  - When should it be accomplished?
  - Who is responsible?
  - How much funding, if any, is required?

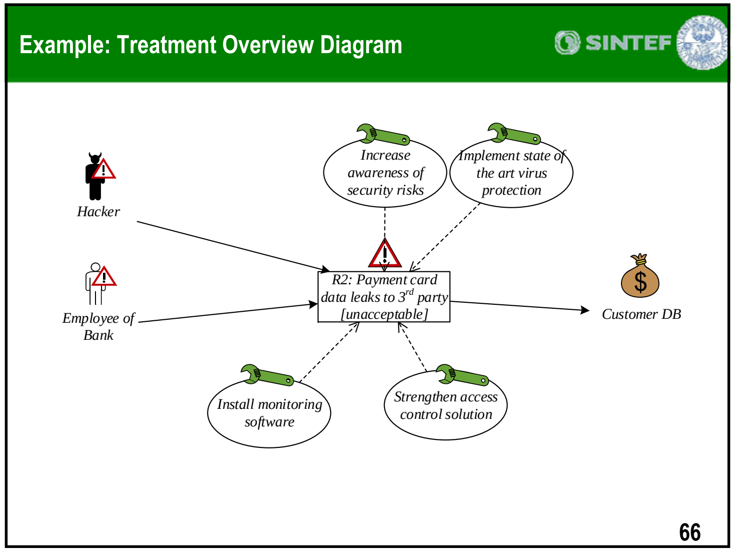
## Identify Treatment – Possible treatments

- Technical treatment: user identification, authentication, authorization, nonrepudiation, transaction privacy, virus detection and eradication,…
- Management treatment : assign security responsibility, security awareness training, periodic system audits, establish incident response capability,…
- Operational treatment : control physical access, secure hub and cable wiring closets, off-site storage procedure, provide an uninterruptible power supply, control temperature and humidity, ensure environmental security,…



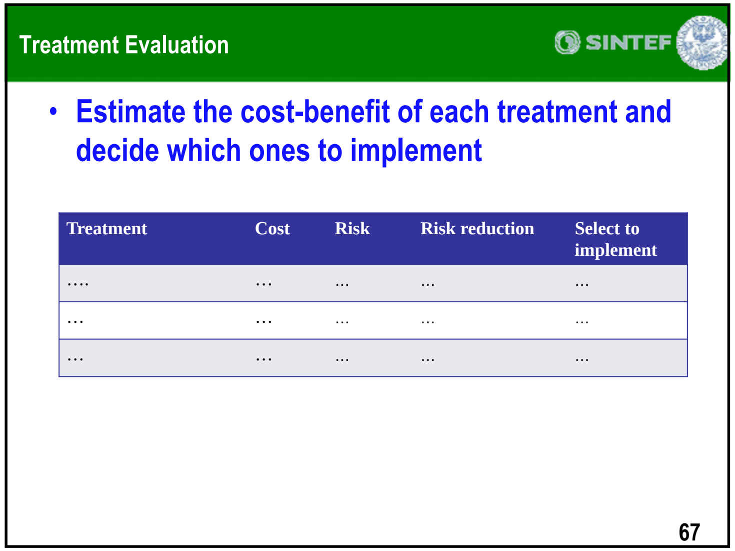
## Example: Treatment Diagram

SINTEF
Strengthen access control solution
Insufficient access control
Hacker breaks into system via remote access pathway [unlikely]
Hacker obtain access to customer DB [rare]
Install monitoring software
Use of remote access
Use of web application
Malcode introduced by hacker via web application [possible]
Implement state of the art virus protection
Hacker
Insufficient virus protection
Malcode causes disclosure of customer data [rare]
R2 : Payment card data leaks to 3rd party
Customer DB
Malcode introduced by hacker via email [unlikely]
Employee of Bank
Work process not aligned with policy
Customer data is by accident sent via email to 3rd party [unlikely]
Lack of competence
Employee stores or transmit customer data on irregular media [possible]
Customer data stored on alternative media by accident disclosed to 3rd party [possible]
Increase awareness of security risks



## Example: Treatment Overview Diagram

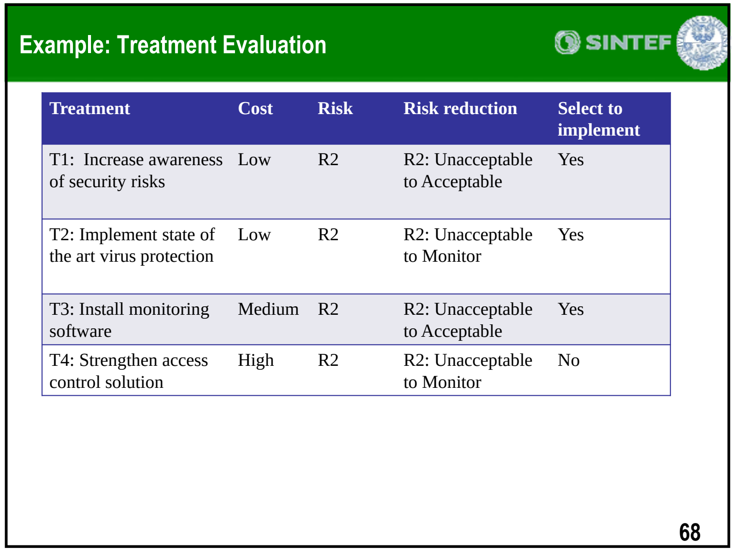
SINTEF
Hacker
Employee of Bank
Increase awareness of security risks
Implement state of the art virus protection
R2: Payment card data leaks to 3rd party [unacceptable]
Customer DB
Install monitoring software
Strengthen access control solution



## Treatment Evaluation

- **Estimate the cost-benefit of each treatment and decide which ones to implement**

| Treatment | Cost | Risk | Risk reduction | Select to implement |
|---|---|---|---|---|
| …. | … | … | … | … |
| … | … | … | … | … |
| … | … | … | … | … |



## Example: Treatment Evaluation

| Treatment | Cost | Risk | Risk reduction | Select to implement |
|---|---|---|---|---|
| T1: Increase awareness of security risks | Low | R2 | R2: Unacceptable to Acceptable | Yes |
| T2: Implement state of the art virus protection | Low | R2 | R2: Unacceptable to Monitor | Yes |
| T3: Install monitoring software | Medium | R2 | R2: Unacceptable to Acceptable | Yes |
| T4: Strengthen access control solution | High | R2 | R2: Unacceptable to Monitor | No |

## Example: Treatment Evaluation

| Treatment | Cost | Risk | Risk reduction | Select to implement |
|---|---|---|---|---|
| T1: Increase awareness of security risks | Low | R2 | R2: Unacceptable to Acceptable | Yes |
| T2: Implement state of the art virus protection | Low | R2 | R2: Unacceptable to Monitor | Yes |
| T3: Install monitoring software | Medium | R2 | R2: Unacceptable to Acceptable | Yes |
| T4: Strengthen access control solution | High | R2 | R2: Unacceptable to Monitor | No |

Residual Risk

## Residual Risk

- Residual Risk – is the risk remaining after the implementation of new or enhanced controls
- If the residual risk has not been reduced to an acceptable level, the risk management cycle must be repeated to identify a way of lowering the residual risk to an acceptable level
- No IT system can be risk-free

## Example: Treatment Evaluation

| Treatment | Cost | Risk | Risk reduction | Select to implement |
|---|---|---|---|---|
| T1: Increase awareness of security risks | Low | R2 | R2: Unacceptable to Acceptable | Yes |
| T2: Implement state of the art virus protection | Low | R2 | R2: Unacceptable to Monitor | Yes |
| T3: Install monitoring software | Medium | R2 | R2: Unacceptable to Acceptable | Yes |
| T4: Strengthen access control solution | High | R2 | R2: Unacceptable to Monitor | No |

Residual Risk

## Treatment Evaluation: Dealing with REALITY

- There’s not enough staff time (human hours) or schedule time or funding to address all potential risks
- Which risks are unacceptable?
- Can we avoid or mitigate these?

Can we live with what we can’t fix?
Will the mitigation strategy work?

## Example: Treatment Evaluation

| Treatment | Cost | Risk | Risk reduction | Select to implement |
|---|---|---|---|---|
| T1: Increase awareness of security risks | Low | R2 | R2: Unacceptable to Acceptable | Yes |
| T2: Implement state of the art virus protection | Low | R2 | R2: Unacceptable to Monitor | Yes |
| T3: Install monitoring software | Medium | R2 | R2: Unacceptable to Acceptable | Yes |
| | | | le | No |

**Final recommendations to customer**

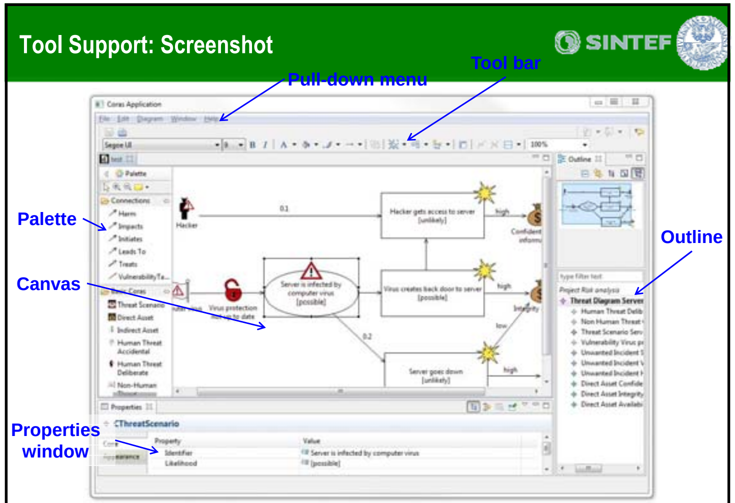
## Contingency Planning

- **Contingency planning:**
  - Only for the most severe risks that **cannot** be mitigated
  - List actions to take should the risk materialize

## Tool Support and Demo

- The CORAS tool is a diagram editor
- Support for making all kinds of CORAS diagrams
- Design for on-the-fly modeling during structured brainstorming at analysis workshops
- Ensures syntactically correct diagrams
- Used during all steps of the risk analysis
  - Input to the various tasks
  - Gathering and structuring of information during the tasks
  - Documentation of analysis results
- Available for download: http://coras.sourceforge.net/

## Tool Support: Screenshot



Pull-down menu

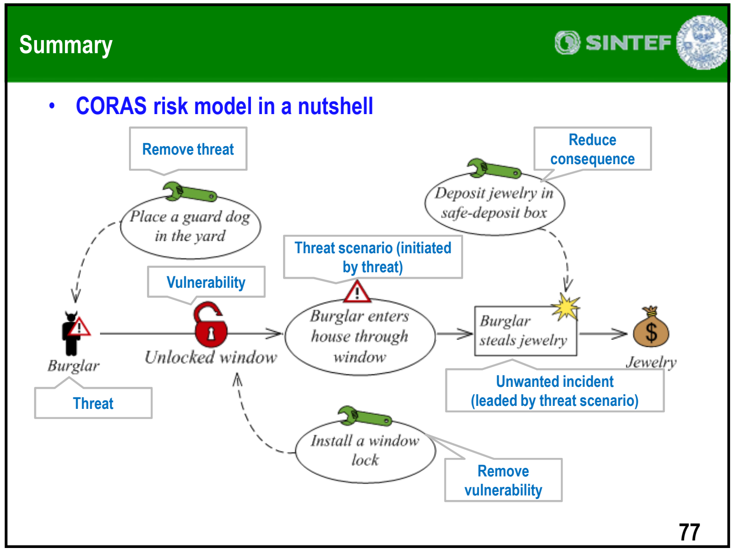
Tool bar

Palette

Canvas

Outline

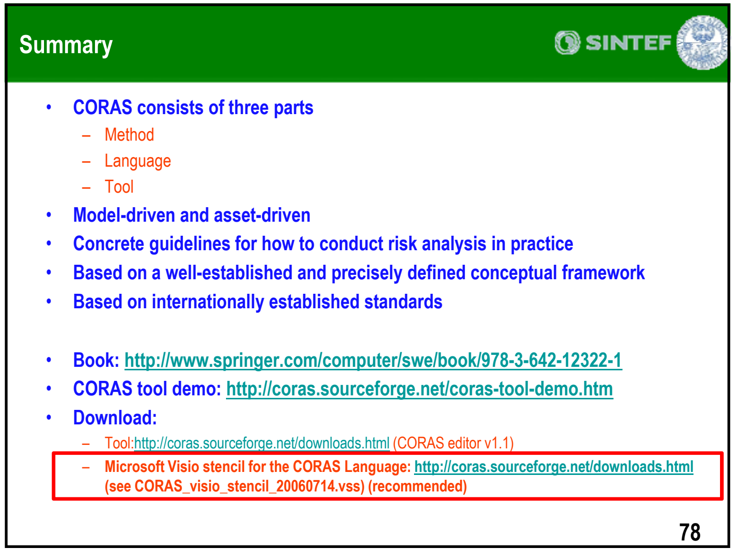
Properties window



## Summary

- CORAS risk model in a nutshell

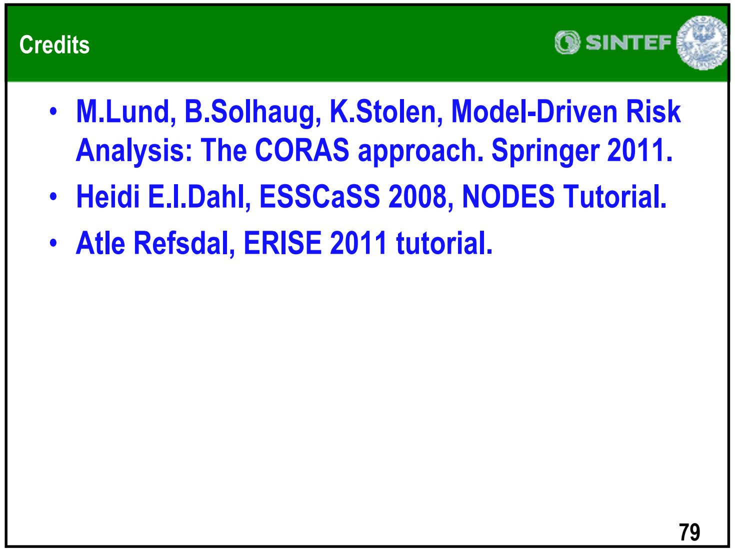
Remove threat
Reduce consequence
Place a guard dog in the yard
Deposit jewelry in safe-deposit box
Threat scenario (initiated by threat)
Vulnerability
Burglar
Unlocked window
Burglar enters house through window
Burglar steals jewelry
$
Jewelry
Threat
Unwanted incident (leaded by threat scenario)
Install a window lock
Remove vulnerability



## Summary

- CORAS consists of three parts
  - Method
  - Language
  - Tool
- Model-driven and asset-driven
- Concrete guidelines for how to conduct risk analysis in practice
- Based on a well-established and precisely defined conceptual framework
- Based on internationally established standards

- Book: http://www.springer.com/computer/swe/book/978-3-642-12322-1
- CORAS tool demo: http://coras.sourceforge.net/coras-tool-demo.htm
- Download:
  - Tool:http://coras.sourceforge.net/downloads.html (CORAS editor v1.1)
  - Microsoft Visio stencil for the CORAS Language: http://coras.sourceforge.net/downloads.html (see CORAS_visio_stencil_20060714.vss) (recommended)



## Credits

- M.Lund, B.Solhaug, K.Stolen, Model-Driven Risk Analysis: The CORAS approach. Springer 2011.
- Heidi E.I.Dahl, ESSCaSS 2008, NODES Tutorial.
- Atle Refsdal, ERISE 2011 tutorial.