Model-Driven Risk Analysis: The CORAS Approach

Le Minh Sang Tran

tran@disi.unitn.it
• What is CORAS?
  – The CORAS approach
  – Central concepts
• Steps of risk analysis in CORAS
• Tool support and Demo
• Summary
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:**
Terms

asset, something of value

vulnerability

threat

constitutes a security risk

we need to introduce security mechanisms

reduced risk level
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

- 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

- Risk management process based on *ISO 31000: Risk Management – Principles and Guidelines*
- Provides *processes and guidelines* for risk analysis
The eight steps of a CORAS risk analysis

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

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
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
AutoParts is a company. Its business is to sell spare parts and accessories for a wide range of car makes and vehicle models.

AutoParts has an automated online store.

AutoParts is distributing catalogues by mail that present its products and is usually shipping the goods to the customers by cash on delivery mail.

AutoParts has decided it wants to do a risk analysis of the system.

Of particular concern for the management is:

- the web application that connects to both their customer database, their inventory database and their online store.
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, their inventory database and their online store.
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 parties
• Identify assets of each party intends to protect:
  – The “THINGS” that are valuable

• Notions to be used in Asset Diagram
Example: Identify Party and Asset

- **Party:**
  - AutoParts company

- **Asset:**
  - Inventory DB
  - Customer DB
  - Online store
  - Compliance
  - Company reputation
  - Customer satisfaction
  - Supplier’s trust
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?  |  What makes this possible?

What does it harm?
## High level Risk analysis

<table>
<thead>
<tr>
<th>Who/ What is the cause?</th>
<th>How? What may happen? What does it harm?</th>
<th>What makes this possible?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hacker</td>
<td>Breaks into system and compromises integrity or confidentiality of databases</td>
<td>Use of web application and remote access; insufficient access control</td>
</tr>
<tr>
<td>Hacker</td>
<td>Attack compromises integrity or confidentiality of personal data causing loss of compliance with data protection laws</td>
<td>Use of web application and remote access; insufficient access control</td>
</tr>
<tr>
<td>Hacker</td>
<td>Introduces virus to the system that compromises integrity or confidentiality of databases</td>
<td>Insufficient virus protection</td>
</tr>
<tr>
<td>Hacker</td>
<td>DoS attack causes online store to go down</td>
<td>Use of web application; insufficient DoS attack prevention</td>
</tr>
</tbody>
</table>
## Example: High level Risk analysis

<table>
<thead>
<tr>
<th>Who/ What is the cause?</th>
<th>How? What may happen?</th>
<th>What makes this possible?</th>
</tr>
</thead>
<tbody>
<tr>
<td>System failure</td>
<td>Online store goes down because of failure of web application or loss of network connection</td>
<td>Immature technology; loss of network connection</td>
</tr>
<tr>
<td>Employee of AutoParts</td>
<td>Collection and processing of personal data diverge from data protection laws</td>
<td>Lack of competence on data protection laws; insufficient routines for processing personal data</td>
</tr>
<tr>
<td>Employee of AutoParts</td>
<td>Sloppiness compromises integrity or confidentiality of databases</td>
<td>Lack of competence; work processes not aligned with policy</td>
</tr>
</tbody>
</table>
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 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**

<table>
<thead>
<tr>
<th>Likelihood</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Certain</td>
<td>Five times or more per year</td>
</tr>
<tr>
<td>Likely</td>
<td>Two to five times per year</td>
</tr>
<tr>
<td>Possible</td>
<td>Once a year</td>
</tr>
<tr>
<td>Unlikely</td>
<td>Less than once per year</td>
</tr>
<tr>
<td>Rare</td>
<td>Less than once per ten years</td>
</tr>
</tbody>
</table>
Define Likelihood scale

- **Example of Likelihood scale**

<table>
<thead>
<tr>
<th>Likelihood</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rarely</td>
<td>A very high number of similar occurrences already on record; has occurred a very high number</td>
</tr>
<tr>
<td>Sometimes</td>
<td>A significant number of similar occurrences already on record; has occurred a significant</td>
</tr>
<tr>
<td>Regularly</td>
<td>Several similar occurrences on record; has occurred more than once</td>
</tr>
<tr>
<td>Often</td>
<td>….</td>
</tr>
<tr>
<td>…</td>
<td>….</td>
</tr>
</tbody>
</table>
Define Consequence scale

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

<table>
<thead>
<tr>
<th>Consequence</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Catastrophic</td>
<td>Range of [50%, 100%] of records are affected</td>
</tr>
<tr>
<td>Serious</td>
<td>Range of [20%, 50%] of records are affected</td>
</tr>
<tr>
<td>Moderate</td>
<td>Range of [10%, 20%] of records are affected</td>
</tr>
<tr>
<td>Minor</td>
<td>Range of [1%, 10%] of records are affected</td>
</tr>
<tr>
<td>Insignificant</td>
<td>Range of [0%, 1%] of records are affected</td>
</tr>
</tbody>
</table>
Define Consequence scale

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

<table>
<thead>
<tr>
<th>Consequence</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Catastrophic</td>
<td>Downtime in range [1 week, ∞&gt;</td>
</tr>
<tr>
<td>Serious</td>
<td>Downtime in range [1 day, 1 week&gt;</td>
</tr>
<tr>
<td>Moderate</td>
<td>Downtime in range [1 hour, 1 day&gt;</td>
</tr>
<tr>
<td>Minor</td>
<td>Downtime in range [1 minute, 1 hour&gt;</td>
</tr>
<tr>
<td>Insignificant</td>
<td>Downtime in range [0, 1 minute&gt;</td>
</tr>
</tbody>
</table>
Define Consequence scale

• **Example of Consequence scale (for direct asset: Customer DB)**

<table>
<thead>
<tr>
<th>Consequence</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Catastrophic</td>
<td>Range of $[50%, 100%]$ of records are affected</td>
</tr>
<tr>
<td>Serious</td>
<td>Range of $[20%, 50%]$ of records are affected</td>
</tr>
<tr>
<td>Moderate</td>
<td>Range of $[10%, 20%]$ of records are affected</td>
</tr>
<tr>
<td>Minor</td>
<td>Range of $[1%, 10%]$ of records are affected</td>
</tr>
<tr>
<td>Insignificant</td>
<td>Range of $[0%, 1%]$ of records are affected</td>
</tr>
</tbody>
</table>
## Define Consequence scale

### Example of Consequence scale (for direct asset: Compliance)

<table>
<thead>
<tr>
<th>Consequence</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Catastrophic</td>
<td>Chief executive officer is sentenced to jail for more than 1 year</td>
</tr>
<tr>
<td>Serious</td>
<td>Chief executive officer is sentenced to jail for up to 1 year</td>
</tr>
<tr>
<td>Moderate</td>
<td>Claim for indemnification or compensation</td>
</tr>
<tr>
<td>Minor</td>
<td>Fine</td>
</tr>
<tr>
<td>Insignificant</td>
<td>Illegal data processing is ordered to cease</td>
</tr>
</tbody>
</table>
Example: Risk Function and evaluation criteria

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

<table>
<thead>
<tr>
<th>Consequence/Likelihood</th>
<th>Insignificant</th>
<th>Minor</th>
<th>Moderate</th>
<th>Serious</th>
<th>Catastrophic</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rare</td>
<td>Green</td>
<td>Green</td>
<td>Yellow</td>
<td>Red</td>
<td>Red</td>
</tr>
<tr>
<td>Unlikely</td>
<td>Green</td>
<td>Green</td>
<td>Yellow</td>
<td>Red</td>
<td>Red</td>
</tr>
<tr>
<td>Possible</td>
<td>Green</td>
<td>Yellow</td>
<td>Red</td>
<td>Red</td>
<td>Red</td>
</tr>
<tr>
<td>Likely</td>
<td>Green</td>
<td>Yellow</td>
<td>Red</td>
<td>Red</td>
<td>Red</td>
</tr>
<tr>
<td>Certain</td>
<td>Green</td>
<td>Red</td>
<td>Red</td>
<td>Red</td>
<td>Red</td>
</tr>
</tbody>
</table>

Acceptable
Monitor
Need to be treated

**Example: Risk Function and evaluation criteria**

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

<table>
<thead>
<tr>
<th>Risk Function (Online Store)</th>
<th>Insignificant</th>
<th>Minor</th>
<th>Moderate</th>
<th>Serious</th>
<th>Catastrophic</th>
</tr>
</thead>
<tbody>
<tr>
<td>Consequence/Likelihood</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Rare</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Unlikely</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Possible</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Likely</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Certain</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Acceptable
Monitor
Need to be treated

Example: Risk Function and evaluation criteria

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

<table>
<thead>
<tr>
<th>Risk Function (Customer DB)</th>
<th>Insignificant</th>
<th>Minor</th>
<th>Moderate</th>
<th>Serious</th>
<th>Catastrophic</th>
</tr>
</thead>
<tbody>
<tr>
<td>Consequence/Likelihood</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Rare</td>
<td>Green</td>
<td>Green</td>
<td>Yellow</td>
<td>Red</td>
<td></td>
</tr>
<tr>
<td>Unlikely</td>
<td>Green</td>
<td>Green</td>
<td>Yellow</td>
<td>Red</td>
<td></td>
</tr>
<tr>
<td>Possible</td>
<td>Green</td>
<td>Yellow</td>
<td>Yellow</td>
<td>Red</td>
<td></td>
</tr>
<tr>
<td>Likely</td>
<td>Yellow</td>
<td>Yellow</td>
<td>Red</td>
<td>Red</td>
<td></td>
</tr>
<tr>
<td>Certain</td>
<td>Yellow</td>
<td>Red</td>
<td>Red</td>
<td>Red</td>
<td></td>
</tr>
</tbody>
</table>

- Acceptable
- Monitor
- Need to be treated

**Example: Risk Function and evaluation criteria**

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

<table>
<thead>
<tr>
<th>Risk Function (Compliance)</th>
<th>Insignificant</th>
<th>Minor</th>
<th>Moderate</th>
<th>Serious</th>
<th>Catastrophic</th>
</tr>
</thead>
<tbody>
<tr>
<td>Consequence/Likelihood</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Rare</td>
<td>Green</td>
<td></td>
<td>Yellow</td>
<td>Yellow</td>
<td>Yellow</td>
</tr>
<tr>
<td>Unlikely</td>
<td>Green</td>
<td>Yellow</td>
<td>Yellow</td>
<td>Red</td>
<td>Red</td>
</tr>
<tr>
<td>Possible</td>
<td>Green</td>
<td>Yellow</td>
<td>Yellow</td>
<td>Red</td>
<td>Red</td>
</tr>
<tr>
<td>Likely</td>
<td>Yellow</td>
<td>Yellow</td>
<td>Red</td>
<td>Red</td>
<td>Red</td>
</tr>
<tr>
<td>Certain</td>
<td>Yellow</td>
<td>Red</td>
<td>Red</td>
<td>Red</td>
<td>Red</td>
</tr>
</tbody>
</table>

- **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”: users/roles inside the system
    - Attackers from outside: “deliberate threat”
Step 5 - sub step 2: Identify Unwanted Incidents

• **Answer the question:**
  – What (unwanted incidents) do we fear will happen?
Step 5 - sub step 2: Identify Unwanted Incidents

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

![Diagram showing identification of unwanted incidents](image)
Step 5 - sub step 2: Identify Unwanted Incidents

- **Answer the question:**
  - What (unwanted incidents) do we fear will happen?
Step 5 - sub step 3: Identify Threat Scenarios

- **Answer the question:**
  - How does it happen? It happens by which threat scenarios?
Step 5 - sub step 3: Identify Threat Scenarios

- **Answer the question:**
  - How does it happen? It happens by which threat scenarios?
Step 5 - sub step 3: Identify Threat Scenarios

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

```
Threat Scenario

Malcode introduced by hacker via web application

Hacker

Malcode introduced by hacker via email

Employee of AutoParts

Malcode causes loss of data on inventory DB

Employee deliberately corrupts integrity of inventory DB

Employee sloppiness compromises integrity of inventory DB

Impact relation

Integrity of inventory DB corrupted

Inventory DB
```
Step 5 - sub step 3: Identify Threat Scenarios

- **Answer the question:**
  - How does it happen? It happens by which threat scenarios?
Step 5 - sub step 3: Identify Threat Scenarios

- Hacker breaks into system via remote access pathway
- Hacker obtains access to DBs
- Hacker initiates DoS attack
- Malcode introduced by hacker via web application
- Virus attacks DB
- Online store down
- Malcode introduced by hacker via email
- Web application goes down
- Loss of network connection
- System failure
- Employee of AutoParts

Online Store
Step 5 - sub step 3: Identify Threat Scenarios

Hacker

- Hacker breaks into system via remote access pathway
- Hacker obtains access to customer DB

Malcode introduced by hacker via web application

Malcode causes disclosure of customer data

Payment card data leaks to 3rd party

Customer DB

Employee of AutoParts

- Malcode introduced by hacker via email
- Customer data is by accident sent via email to 3rd party

Employee stores or transmit customer data on irregular media

Customer data stored on alternative media by accident disclosed to 3rd party

Personal identifiable information leaks to 3rd party

Compliance

[$]
Step 5 - sub step 4: Identify Vulnerabilities

• Answer the question:
  – Which vulnerabilities make this possible?
Step 5 - sub step 4: Identify Vulnerabilities

- Answer the question:
  - Which vulnerabilities make this possible?
Step 5 - sub step 4: Identify Vulnerabilities

1. Hacker breaks into system via remote access pathway
2. Hacker initiates DoS attack
3. Insufficient DoS prevention
4. Hacker obtains access to DBs
5. Use of remote access
6. Use of web application
7. Insufficient virus protection
8. Malcode introduced by hacker via web application
9. Malcode introduced by hacker via email
10. Work process not aligned with policy
11. Employee of AutoParts
12. Immature technology
13. Web application goes down
14. Loss of network connection
15. System failure
16. Unstable network connection
17. Online store down
18. Online Store
Step 5 - sub step 4: Identify Vulnerabilities

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

- **Hacker**
  - Use of web application
  - Malcode introduced by hacker via web application (possible)
    - Malcode causes loss of data on inventory DB (unlikely)
      - Integrity of inventory DB corrupted (unlikely)
        - Serious
          - Inventory DB

- **Employee of AutoParts**
  - Use of web application
  - Insufficient screening
    - Employee deliberately corrupts integrity of inventory DB (rare)
  - Lack of competence
    - Employee sloppiness compromises integrity of inventory DB (likely)
Example: Assign Likelihood and Consequence
Example: Assign Likelihood and Consequence

- Hacker breaks into system via remote access pathway [unlikely]
- Insufficient access control
- Use of remote access

- Hacker obtains access to customer DB [rare]
- Malcode introduced by hacker via web application [possible]
- Insufficient virus protection

- Payment card data leaks to 3rd party [rare]

- Malcode causes disclosure of customer data [rare]

- Customer data is by accident sent to 3rd party [unlikely]
- Lack of competence

- Employee stores or transmit customer data on irregular media [possible]
- Employee of AutoParts

- Work process not aligned with policy

- Personal identifiable information leaks to 3rd party [possible]

- Customer data stored on alternative media by accident disclosed to 3rd party [possible]

- Compliance

- Catastrophic

- Moderate

- Minor
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
### Risk Function (Inventory DB)

<table>
<thead>
<tr>
<th>Consequence/Likelihood</th>
<th>Insignificant</th>
<th>Minor</th>
<th>Moderate</th>
<th>Serious</th>
<th>Catastrophic</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rare</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Unlikely</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Possible</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Likely</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Certain</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- **Acceptable**: Green
- **Monitor**: Yellow
- **Need to be treated**: Red

*R1: Integrity of inventory DB corrupted*
## Example: Completed Risk Function

### Risk Function (Online Store)

<table>
<thead>
<tr>
<th>Consequence/Likelihood</th>
<th>Insignificant</th>
<th>Minor</th>
<th>Moderate</th>
<th>Serious</th>
<th>Catastrophic</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rare</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Unlikely</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Possible</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Likely</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Certain</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Consequence/Likelihood
- Insignificant
- Minor
- Moderate
- Serious
- Catastrophic

### Likelihood
- Rare
- Unlikely
- Possible
- Likely
- Certain

### Risk Assessment
- Green = Acceptable
- Yellow = Monitor
- Red = Need to be treated

Example: R2: Online store down
## Example: Completed Risk Function

<table>
<thead>
<tr>
<th>Risk Function (Customer DB)</th>
<th>Consequence/Likelihood</th>
<th>Insignificant</th>
<th>Minor</th>
<th>Moderate</th>
<th>Serious</th>
<th>Catastrophic</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rare</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>R3: Payment card data leaks to 3rd party</td>
</tr>
<tr>
<td>Unlikely</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Possible</td>
<td></td>
<td></td>
<td></td>
<td>R4: Personal identifiable information leaks to 3rd party</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Likely</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Certain</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- **Acceptable**: Green
- **Monitor**: Yellow
- **Need to be treated**: Red
### Example: Completed Risk Function

<table>
<thead>
<tr>
<th>Risk Function (Compliance)</th>
<th>Consequence/Likelihood</th>
<th>Insignificant</th>
<th>Minor</th>
<th>Moderate</th>
<th>Serious</th>
<th>Catastrophic</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rare</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Unlikely</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Possible</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Need to be treated</td>
</tr>
<tr>
<td></td>
<td>R5: Personal identifiable information leaks to 3(^{rd}) party</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Likely</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Certain</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- **Green**: Acceptable
- **Yellow**: Monitor
- **Red**: 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

RI: Integrity of inventory DB corrupted [unacceptable]

R2: Online store down [monitor]

R3: Payment card data leaks to 3rd party [unacceptable]

R4: Personal identifiable information leaks to 3rd party [monitor]

R5: Personal identifiable information leaks to 3rd party [acceptable]

Inventory DB

Online Store

Customer DB

Customer satisfaction

Reputation

Compliance

Sub-supplier's trust

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
Example: Treatment Diagram

1. **Hacker**
   - Use of remote access
   - Hacker breaks into system via remote access pathway [unlikely]

2. **Employee of AutoParts**
   - Employee stores or transmits customer data on irregular media [possible]
   - Work process not aligned with policy

3. **Malware introduced by hacker via email [unlikely]**
   - Employee data is by accident sent via email to 3rd party [unlikely]
   - Lack of competence

4. **Employee data is by accident disclosed to 3rd party [possible]**
   - Increase awareness of security risks

5. **Malware causes disclosure of customer data [rare]**
   - Insufficient virus protection

6. **Customer data leaks to 3rd party**
   - Customer DB

7. **Hacker obtains access to customer DB [rare]**
   - Insufficient access control

8. **Install monitoring software**
   - Strengthen access control solution

- General Recommendations:
  - Implement state of the art virus protection
  - Increase awareness of security risks
  - Strengthen access control solution
Example: Treatment Overview Diagram

R1: Integrity of inventory DB corrupted [unacceptable]

- Hacker

R3: Payment card data leaks to 3rd party [unacceptable]

- Employee of AutoParts

Implement new, secure backup solution

Increase awareness of security risks

Implement state of the art virus protection

Install monitoring software

Strengthen access control solution

Inventory DB

Customer DB
• Estimate the cost-benefit of each treatment and decide which ones to implement

<table>
<thead>
<tr>
<th>Treatment</th>
<th>Cost</th>
<th>Risk</th>
<th>Risk reduction</th>
<th>Select to implement</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
## Example: Treatment Evaluation

<table>
<thead>
<tr>
<th>Treatment</th>
<th>Cost</th>
<th>Risk</th>
<th>Risk reduction</th>
<th>Select to implement</th>
</tr>
</thead>
<tbody>
<tr>
<td>T1: Implement new, secure backup solution</td>
<td>High</td>
<td>R1</td>
<td>R1: Unacceptable to Acceptable</td>
<td>No</td>
</tr>
<tr>
<td>T2: Increase awareness of security risks</td>
<td>Low</td>
<td>R1</td>
<td>R1: Unacceptable to Monitor</td>
<td>Yes</td>
</tr>
<tr>
<td>T3: Implement state of the art virus protection</td>
<td>Low</td>
<td>R1</td>
<td>R1: Unacceptable to Monitor</td>
<td>Yes</td>
</tr>
<tr>
<td>T4: Install monitoring software</td>
<td>Medium</td>
<td>R3</td>
<td>R3: Unacceptable to Acceptable</td>
<td>Yes</td>
</tr>
<tr>
<td>T5: Strengthen access control solution</td>
<td>High</td>
<td>R3</td>
<td>R3: Unacceptable to Monitor</td>
<td>No</td>
</tr>
</tbody>
</table>
### Example: Treatment Evaluation

<table>
<thead>
<tr>
<th>Treatment</th>
<th>Cost</th>
<th>Risk</th>
<th>Risk reduction</th>
<th>Select to implement</th>
</tr>
</thead>
<tbody>
<tr>
<td>T1: Implement new, secure backup solution</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>T2: Increase awareness of security risks</td>
<td>Low</td>
<td>R1</td>
<td>R1: Unacceptable to Monitor</td>
<td>Yes</td>
</tr>
<tr>
<td>T3: Implement state of the art virus protection</td>
<td>Low</td>
<td>R1</td>
<td>R1: Unacceptable to Monitor</td>
<td>Yes</td>
</tr>
<tr>
<td>T4: Install monitoring software</td>
<td>Medium</td>
<td>R3</td>
<td>R3: Unacceptable to Acceptable</td>
<td>Yes</td>
</tr>
<tr>
<td>T5: Strengthen access control solution</td>
<td>High</td>
<td>R3</td>
<td>R3: Unacceptable to Monitor</td>
<td>No</td>
</tr>
</tbody>
</table>

**Final recommendations to customer:**

- T2: Increase awareness of security risks - Yes
- T3: Implement state of the art virus protection - Yes
- T4: Install monitoring software - Yes
- T5: Strengthen access control solution - No
• 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/
• CORAS risk model in a nutshell

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

Threat scenario (initiated by threat)
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

- Download:
  - Microsoft Visio stencil for the CORAS Language: [http://coras.sourceforge.net/downloads.html](http://coras.sourceforge.net/downloads.html) (see CORAS_visio_stencil_20060714.vss) (recommended)
• Atle Refsdal, ERISE 2011 tutorial.
From Treatments to Security Requirements
• **Security goal:**
  – is an expression of the need to protect an asset from harm

• **Security requirements:**
  – are functional or non-functional requirements that need to be satisfied in order to achieve the security goals on a system
• **Security control:**
  - is safeguard or countermeasure to avoid, counteract or minimize the risks on the assets
  - By implementing the security controls, the security requirements can be satisfied, and hence, also the security goals

• **Types of security controls:**
  - Physical controls:
    - Example: guard dog, fences, doors, locks, fire extinguishers,…
  - Procedure controls
    - Example: security awareness and training, incident response processes, management oversight,…
  - Technical controls:
    - Example: access controls, antivirus software, firewall, user authentication …
  - Legal and regulatory or compliance controls:
    - Example: privacy laws, policies and clauses

• **The treatments in CORAS can be considered as security controls**
From Risks to Security goals

- **Identify security goals from (unacceptable) risks**
- **Example**

<table>
<thead>
<tr>
<th>Risks</th>
<th>Asset that is harmed</th>
<th>Security Goals</th>
</tr>
</thead>
<tbody>
<tr>
<td>R1: Integrity of inventory DB corrupted</td>
<td>Inventory DB</td>
<td>SG1: The inventory DB needs to be properly protected from flaw manipulations</td>
</tr>
<tr>
<td>R3: Payment card data leaked to 3\textsuperscript{rd} party</td>
<td>Customer DB</td>
<td>SG2: the customer DB needs to be properly protected from the leakage</td>
</tr>
</tbody>
</table>

- **Note:** the number of security goals may not need to be identical with the number of risks (i.e., you can have 5 risks, and 3 security goals, or vice versa)
• Identify security requirements from treatments.
• These security requirements can be satisfied by implementing proper treatments
• The security goals are hence achieved when the security requirements are satisfied
Example (for all treatments, also including the ones which are finally not recommended to the customer):

<table>
<thead>
<tr>
<th>Treatments (Security controls)</th>
<th>Security Requirements</th>
<th>Security Goals</th>
</tr>
</thead>
<tbody>
<tr>
<td>T1: Implement new, secure backup solution</td>
<td>SR1: The Online Store system should have the backup mechanism for any database</td>
<td>SG1</td>
</tr>
<tr>
<td>T2: Increase awareness of security risks</td>
<td>SR2: The employee of Online Store should have a proper background, in a security sense, relating to their tasks in the company</td>
<td>SG1, SG2</td>
</tr>
<tr>
<td>T3: Implement state of the art virus protection</td>
<td>SR3: The Online Store system should be able to detect any malicious code or malicious software</td>
<td>SG1, SG2</td>
</tr>
<tr>
<td>T4: Install monitoring software</td>
<td>SR4: The database and web application of Online Store should be monitored and scanned to ensure no suspicious activity, tampering or malicious software</td>
<td>SG2</td>
</tr>
<tr>
<td>T5: Strengthen access control solution</td>
<td>SR5: The Online Store system should have a proper access control mechanism to ensure for authentication and authorization</td>
<td>SG2</td>
</tr>
</tbody>
</table>

Note: the number of security requirements may not need to be identical with the number of treatments (i.e., you can have more security requirements than treatments, or vice versa.)
- One treatment can be implemented to satisfy more than one security requirement(s)
- One security requirement can be satisfied by implementing more than one treatment(s)
More examples on CORAS diagrams
More example

• Asset Diagram

Company

Party

Indirect asset

Harm relation

Asset

Company’s reputation

Integrity of server [high]

Confidentiality of information [critical]

Availability of server [critical]
• Threat Diagram

- Virus protection not up to date
- Computer virus
  - Server is injected by computer virus [possible]
  - The virus is an email worm overloading the email server [possible]
  - The virus is a SQL worm overloading the SQL server [unlikely]
- Virus creates back door to server [possible]
- Server goes down [unlikely]
  - Integrity of server high
  - Availability of server high
• Risk Diagram

VB: Virus creates back door to server [unacceptable]

SD2: Server goes down [acceptable]

Computer virus

Initiates relation

Risk

Initiates relation

Risk level

Integrity of server

Availability of server

Impacts relation

Availability of server

>>>
Note: it may not be required to specify the treatment category in this diagram.
More example

• **Treatment Overview Diagram**

- Install monitoring software
- Reduce consequence
- Treats relation
- Hacker

- HA: Hacker gets access to server [unacceptable]
- Confidentiality of information

- Vb: Virus creates back door to server [unacceptable]

- Computer virus
- Reduce likelihood

- SD2: Server goes down [acceptable]
  - Integrity of server

- SD1: Server goes down [unacceptable]
  - Availability of server

- Implement new routines for updating virus protection
More Example

- "initiate" to Alice's sister runs file sharing application on home laptop
- "leads to" Hacker gains access to Alice's laptop
- "leads to" Hacker copies all data from laptop
- "leads to" Hacker deletes all files in "My Documents"
- "leads to" Spyware crashes computer
- "leads to" Computer component fails
- "leads to" All work of thesis is lost
- "leads to" A day's worth of work in the thesis is lost

"impact" to Competitor uses business sensitive information strategically
- "leads to" Business sensitive information is published in national newspaper
- "leads to" PhD thesis

"initiate" to "leads to" Alice installs software that contains spyware on her laptop
- "leads to" Spyware crashes computer
- "leads to" Computer component fails
- "leads to" All work of thesis is lost
- "leads to" A day's worth of work in the thesis is lost
“vulnerability target”

Alice's sister runs file sharing application on home laptop

Alice's sister shares folder with business sensitive information

Hacker gains access to Alice's laptop

Hacker deletes all files in "My Documents"

Spyware crashes computer

Computer component fails

Hacker copies all data from laptop

Business sensitive information is published in national newspaper

Competition uses business sensitive information strategically

Alice's reputation

BC's reputation

Compliance with contract between Alice and BC

All work of thesis is lost

A day's worth of work in the thesis is lost

PhD thesis

No backup for thesis files

Old components

Unaware of spyware

No firewall

Complicated file sharing preferences

Home laptop

Alice installs software that contains spyware on her laptop

"vulnerability target"
More example: Assign Likelihood and Consequence

Competitor uses business sensitive information strategically [rarely]

Business sensitive information is published in national newspaper [rarely]
More example: Assign Likelihood and Consequence
Risk Matrix
(PhD thesis)

<table>
<thead>
<tr>
<th>Consequence/ Likelihood</th>
<th>Insignificant</th>
<th>Minor</th>
<th>Moderate</th>
<th>Serious</th>
<th>Catastrophic</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rarely</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Unlikely</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Possible</td>
<td></td>
<td></td>
<td>A day’s worth of work on the thesis is lost</td>
<td>All work on thesis is lost</td>
<td></td>
</tr>
<tr>
<td>Likely</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Certain</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Risk Matrix
(Business sensitive information)

<table>
<thead>
<tr>
<th>Consequence/Likelihood</th>
<th>Insignificant</th>
<th>Minor</th>
<th>Moderate</th>
<th>Serious</th>
<th>Catastrophic</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rarely</td>
<td></td>
<td></td>
<td></td>
<td>Business sensitive information is published in national newspaper</td>
<td>Competitors uses Business sensitive information strategically</td>
</tr>
<tr>
<td>Unlikely</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Possible</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Likely</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Certain</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
More example: Risk diagram

R1: Competitors uses business sensitive information strategically [need to be treated]

R2: Business sensitive information is published in national newspaper [monitor]

R3: All work in the thesis is lost [need to be treated]

R4: A day’s worth of work on the thesis is lost [monitor]
More example: Treatment Overview Diagram

Treatment Overview Diagram for R1 and R3

R1: Competitors uses business sensitive information strategically [need to be treated]

- Alice's sister
- Hacker
- Install firewall

R3: All work in the thesis is lost [need to be treated]

- Alice
- Home laptop
- Spyware awareness course
- Do regular backup of thesis files

Restrict sharing on home laptop

- BC's reputation
- Alice's reputation
- Compliance with contract between BC and Alice

Business sensitive information

- $