Pattern-Based and ISO 27001 Compliant Risk Analysis for Cloud Systems

Azadeh Alebrahim[1], Ludger Goeke[2], Denis Hatebur[1,2]

(1) University of Duisburg-Essen, Germany
(2) ITESYS Institute for technical Systems GmbH, Germany

funded by Ziel2.NRW

August 25, 2014

Context

- Small and medium enterprises (SMEs)
- Cloud computing services
- Security is important for cloud customers
- Certification of applied security mechanisms
- ISO 27001 (tailoring)
- Research project ClouDAT (`http://www.cloudat.de`)

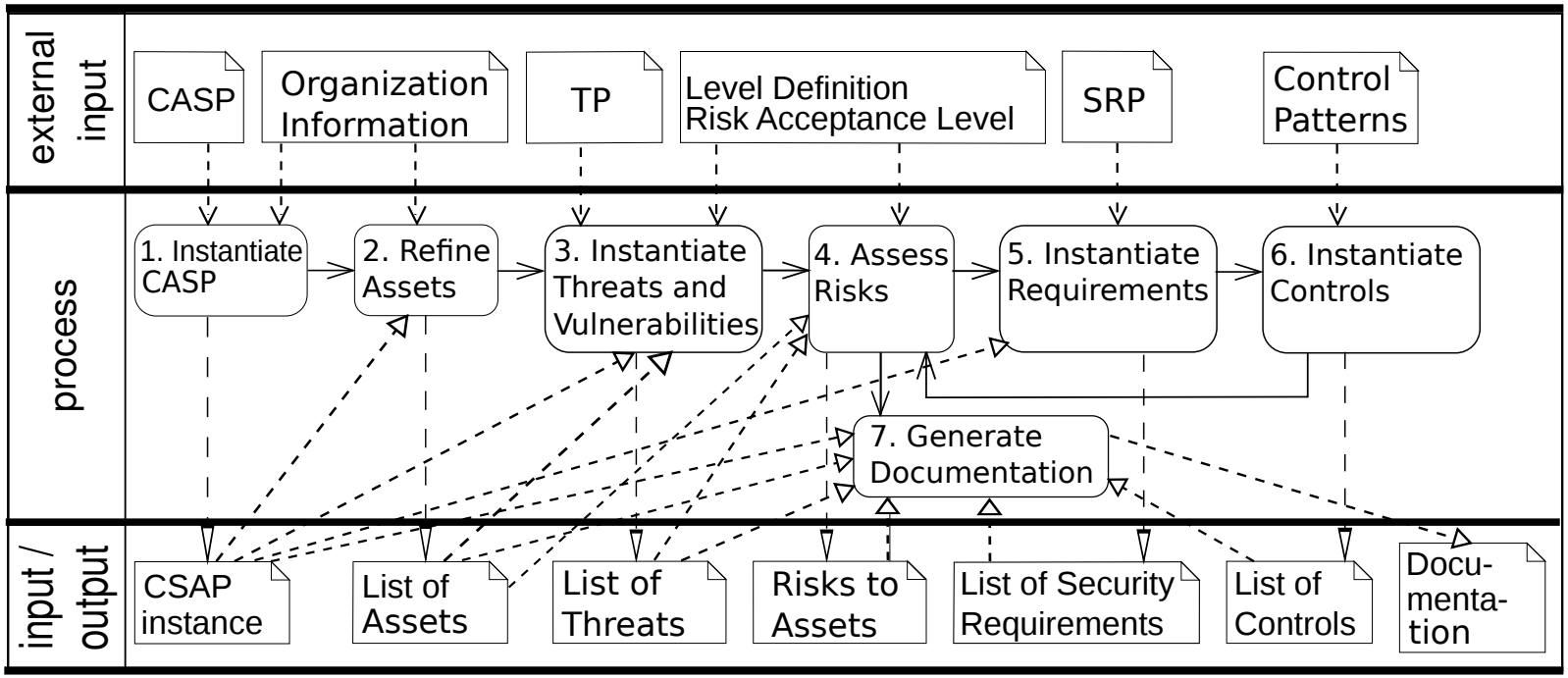
ISO 27001

- For certifying cloud computing systems, we selected ISO 27001.
- It provides general concepts for establishing information security risk management.
- ISO 27001:2013: less details on processes than in ISO 27001:2005
- ISO 27001:2013: processes of ISO 27001:2005 are sufficient

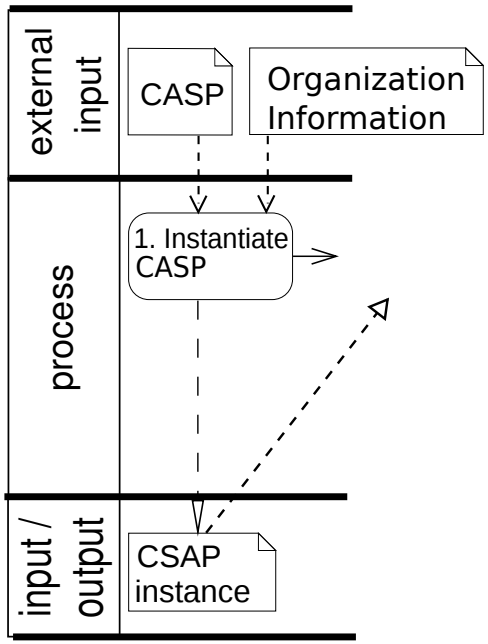
Problem

- Idea is to create a documentation of the cloud system using patterns and a defined process.
- The risk analysis is an essential element of this documentation.
- The ISO 27001 does not stipulate any method for performing risk analysis.

How to tackle the problem? Method Overview

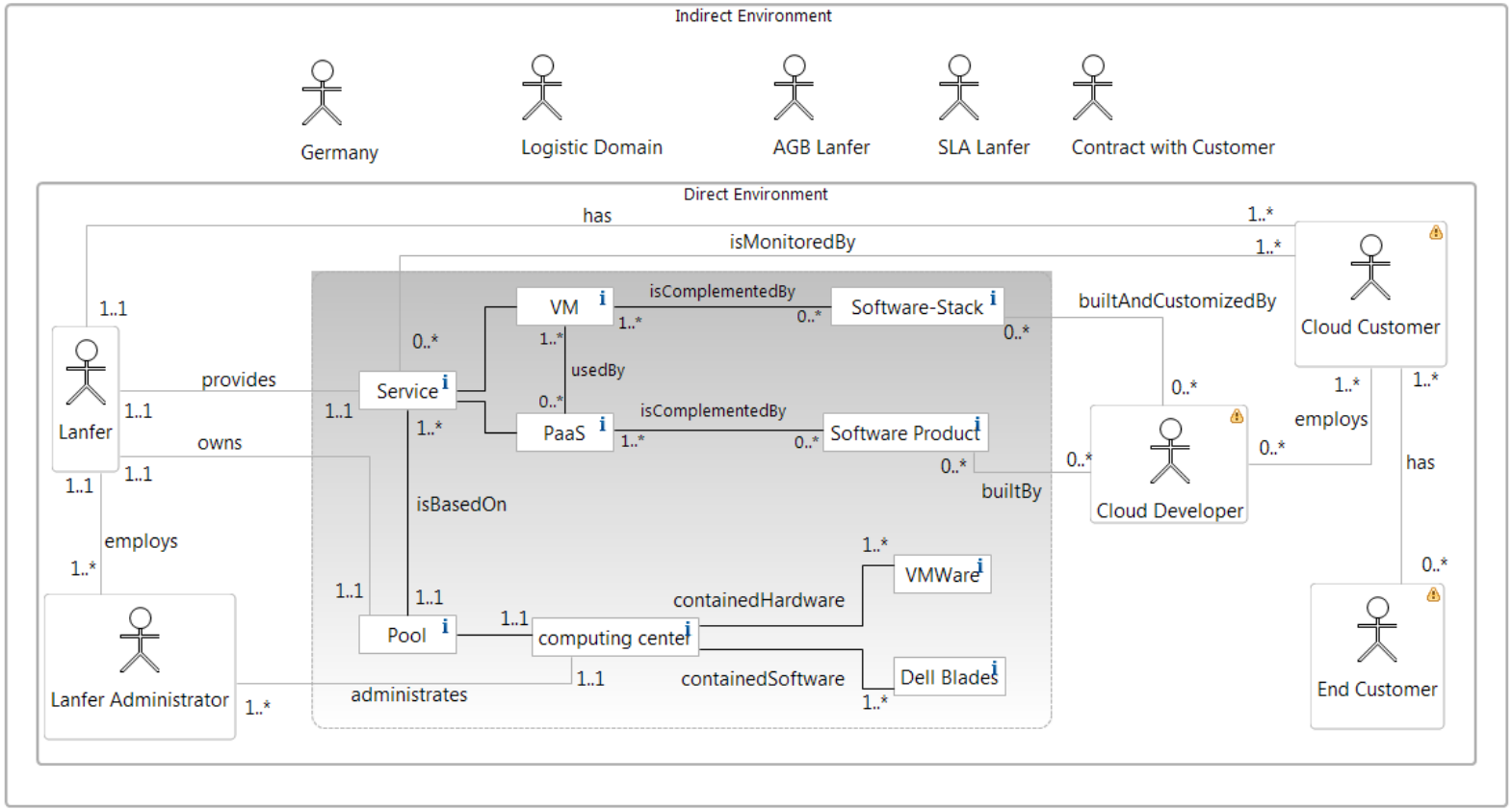


Phase 1: Instantiate CSAP

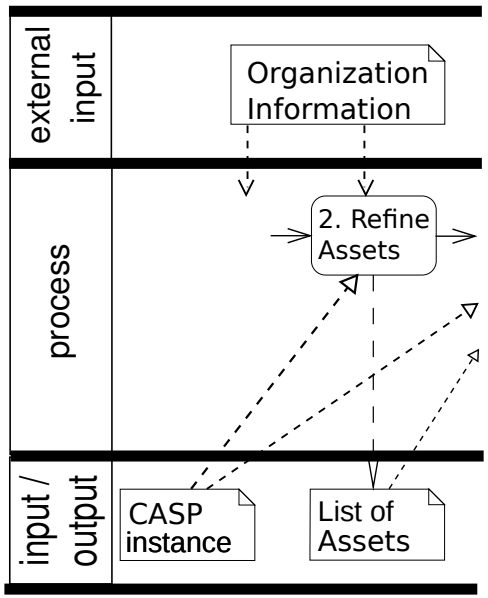


- Cloud System Analysis Pattern (CSAP)
- CSAP was introduced in *[Beckers2011]*x.
- CSAP is used to describe context and scope

Phase 1: CSAP instance example

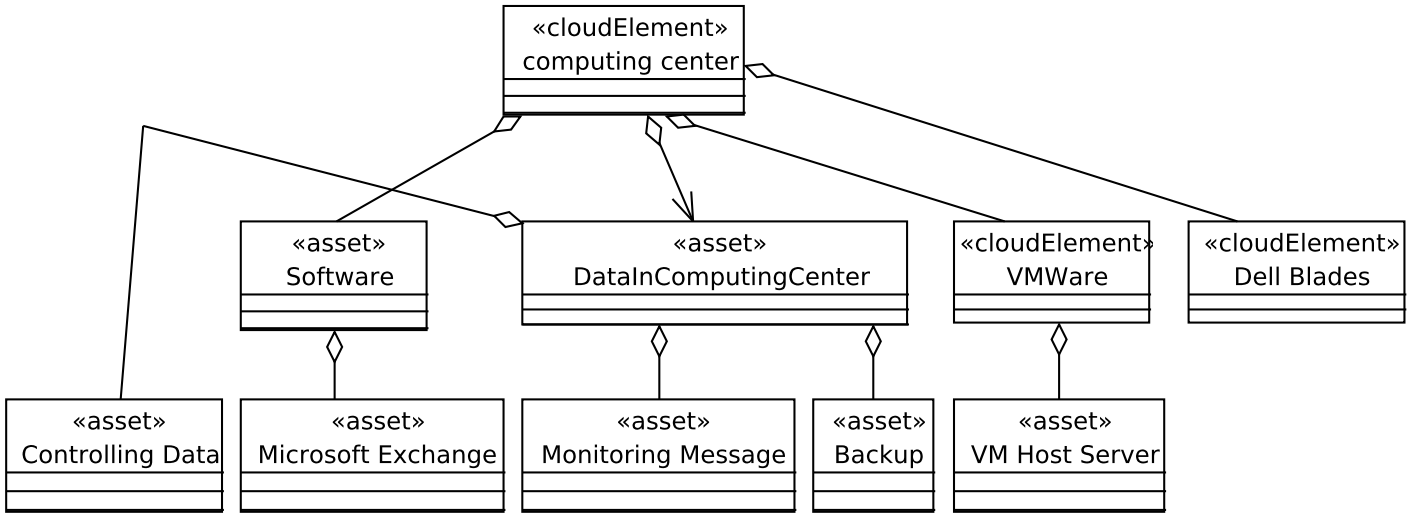


Phase 2: Refine Assets

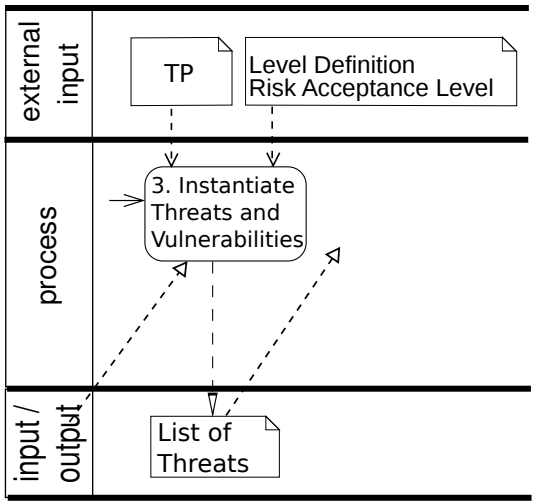


Refines the CloudElements of the CSAP instance
e.g. by specialization or composition.

Phase 2: Asset examples



Phase 3: Instantiate threats and vulnerabilities



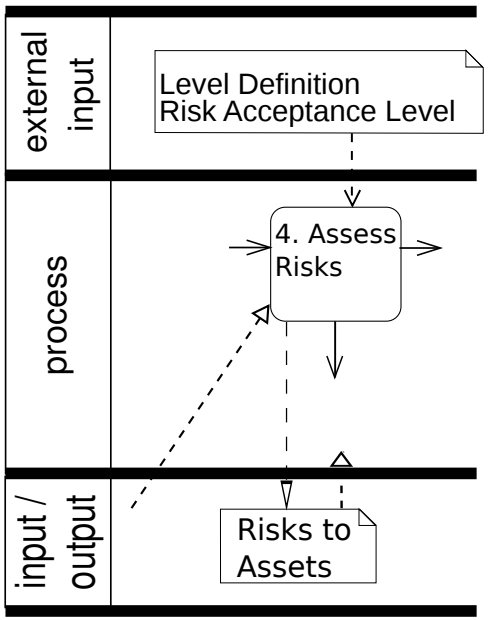
- For all identified assets, threats and maybe vulnerabilities are identified
- Threat patterns (TP) are instantiated according to CSAP instance and refined assets

Phase 3: Threat example

An excerpt of identified assets, related threats, and vulnerabilities

Asset label	**Threat (C)**	**Threat (I)**	**Threat (A)**	**Vulnerability**
Controlling Data	Disclosure of stored *Controlling Data* of *LANFER SYSTEMHAUS* by *an attacker*	Modification of *Controlling Data* by an attacker	Unavailability of *Controlling Data* for *LANFER SYSTEMHAUS*	e.g., gaining access to secured area (C,I,A)
Microsoft Exchange	-	Modification of *Microsoft Exchange* by *an attacker*	Unavailability of *Microsoft Exchange* for *LANFER SYSTEMHAUS*	e.g., impersonate an administrator and install modified Exchange software (I)
Monitoring Message	Disclosure of communication between *virtual machine* and *employees*	Modification of communication between *virtual machine* and *employees* to modify *Monitoring Message*	Unavailability of communication between *virtual machine* and *employees*	e.g., network sniffing to read monitoring messages (C)
Backup	Disclosure of stored *backup* of *LANFER SYSTEMHAUS* by *an attacker*	Modification of *Backup* by an attacker	Unavailability of *backup* for *LANFER SYSTEMHAUS*	e.g., responsible person and all representatives are not available when access to backup is necessary (A)
VM Host Server	-	Modification of *VM Host Server* by an attacker	Unavailability of *VM Host Server* for *LANFER SYSTEMHAUS*	e.g., gaining access to secured area (I,A)

Phase 4: Assess Risks



- A risk evaluation method with defined risk levels and a risk acceptance level is used.
- For all identified assets, risks are rated according to given threats, vulnerabilities and controls.
- As long as one risk rating is above the risk acceptance level, the process is continued.
- When all risk ratings are below the risk acceptance level, the final documentation for certification can be generated.

Phase 4: Risk level definition

Impact value scale (consequence scale)

Impact value	**Description**
1	no consequence if asset is successfully threatened
2	consequence can be easily handled
3	to handle consequences moderate effort is necessary
4	to handle consequences high effort is necessary
5	company survival uncertain if asset is successfully threatened

Security failure likelihood scale (VL:Vulnerability Level, TL: Threat Likelihood)

Security failure	**(VL, TL)**	**Description**
1	(L,LOW)	Almost no vulnerability because all identified threats are addressed by controls and attackers have only minor interest
2	(M,LOW)	Basic protection is given and attackers have only minor interest
3	(H,LOW) or (L,HIGH)	Possible threats are not addressed by controls and attackers have only minor interest/ Almost no vulnerability because all identified threats are addressed by controls and attackers have an interest to threaten asset
4	(M,HIGH)	Basic protection is given and attackers have an interest to threaten asset
5	(H,HIGH)	Possible threats are not addressed by controls and attackers have an interest to threaten asset

Acceptance level: 8

Phase 4: Risk example

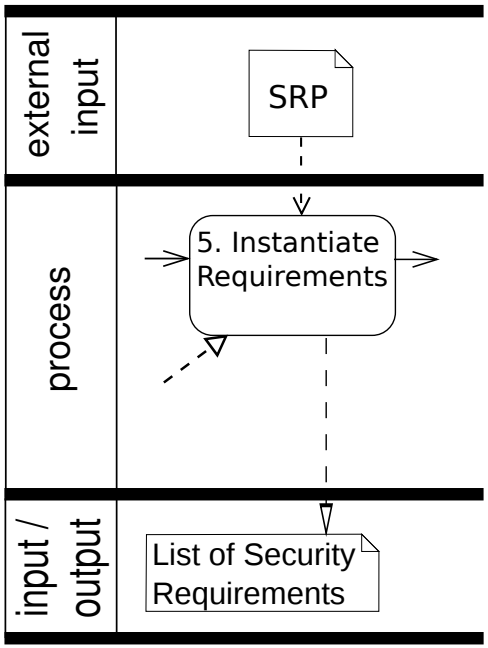
Business impact (B.I.), likelihoods for security failures (S.F.), and the estimated risk level (R.L.) for identified assets

Asset label	**B.I (C)**	**B.I (I)**	**B.I (A)**	**S.F. (C)**	**S.F. (I)**	**S.F. (A)**	**R.L. (C)**	**R.L. (I)**	**R.L. (A)**
Controlling Data	4	3	2	3	2	2	12	6	4
Microsoft Exchange	-	2	3	-	2	2	-	4	4
Monitoring Message	2	2	2	2	5	3	4	10	6
Backup	2	2	3	3	2	1	6	4	3
VM Host Server	-	1	5	-	3	3	-	-	15

The ISO 27001 specifies the following treatments:

1. applying appropriate controls
2. accepting risks
3. avoiding risks
4. transferring the associated business risks to other parties

Phase 5: Instantiate Requirements



- According to the threats, useful requirement patterns are suggested.
- Requirement patterns are instantiated using the instantiation of the threats.

Phase 5: Instantiated Requirements

SR 1 Preserve confidentiality of stored *controlling data* of the *LANFER SYSTEMHAUS* by preventing disclosure by *an attacker*.

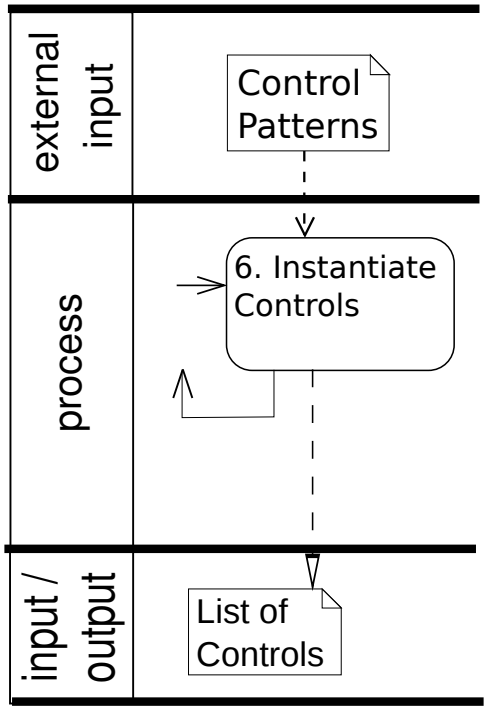
SR 2 The integrity of communication between *virtual machine* and *employees* shall be preserved.

SR 3 Manipulation on *VM host server* that leads to the unavailability of it shall be prevented.

SR 4 Sufficient physical protection shall be implemented (no windows in ground floor, access control for all entries with limited access for visitors, . . .) to ensure availability regarding the *VM host server*.

SR 5 Technical malfunctions of the *VM host server* shall not affect the availability of the *provided platform*.

Phase 6: Instantiate Controls



- According to the requirement, according to predefined dependencies, useful control patterns are suggested.
- After instantiation of controls, remaining risks are assessed.

Phase 6: Instantiated Controls

C 1 To address security requirement *SR 1*, we apply the controls of ISO 27002:2013, e.g., equipment security (A.11.2), access control (A.9) including the controls according to our mapping, e.g. human resource security (A.7).

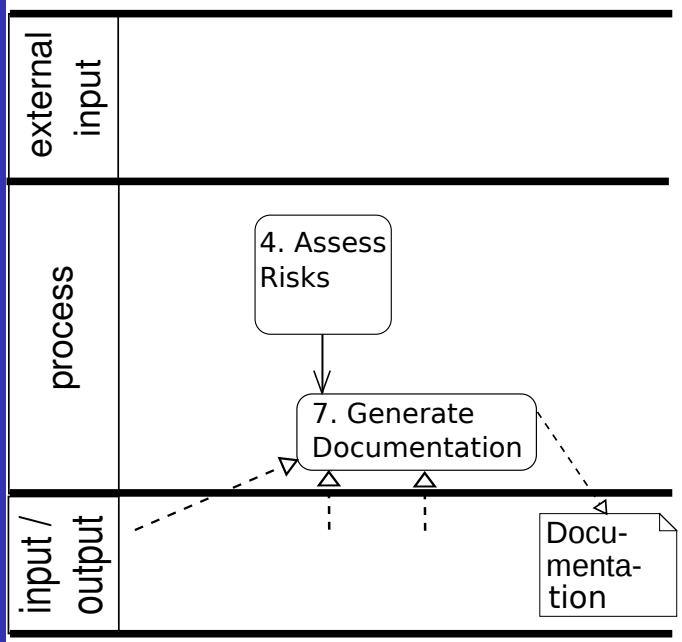
C 2 To address security requirement *SR 2*, cryptographic means for signatures were applied including the necessary measures from ISO 27002:2013 (A.10).

C 3 To address security requirement *SR 3*, we apply the same controls as for the security requirement *SR 1*. In addition, we apply control A.11.1.

C 4 Controls addressing security requirement *SR 4* (e.g. A.11.1) were already in place.

C 5 To address security requirement *SR 5*, controls for redundant servers (A.17.2) have to be applied.

Phase 7: Generate Documents



- When all risk ratings are below the the risk acceptance level, the final documentation for certification can be generated.
- The generated documentation generally fulfills the ISO 27001 requirements.
- It can be used for certification.
- All artifacts from previous steps are used.

Conclusion

- Structured method to perform an ISO 27001 compliant risk analysis
- Using Patterns to reduce effort and use existing knowledge:
  - context and structure with CSAP
  - security requirements with SRP
  - threats with TP
  - controls with CP
- Systematic pattern-based identification of
  - threats using TP and their relationship to CSAP elements
  - security requirements to be fulfilled by appropriate controls using SRP and their relationship to TP
  - controls using CP and their relationship to SRP

Future Work

- SaaS and PaaS risk analysis started
- Later phases of ISO 27001
- Improved and completed tool support including validation steps