# D2.2
# System and dependency analysis (second iteration) – Pilot scenario definition


| | |
|---|---|
| Grant Agreement number: | 740723 |
| Project acronym: | CS-AWARE |
| Project title: | A cybersecurity situational awareness and information sharing solution for local public administrations based on advanced big data analysis |



| | |
|---|---|
| Principal author: | Thomas Schaberreiter, University of Vienna, thomas.schaberreiter@univie.ac.at<br>Christopher C. Wills, Caris Research, ccwills@carisresearch.co.uk |
| Co-author(s) | Jerry Andriessen, Wise&Munro<br>Konstantinos Rantos, InnoSec<br>Arnold Spyros, InnoSec<br>Alex Papanikolaou, InnoSec<br>Veronika Kupfersberger, University of Vienna<br>Gregor Langner, University of Vienna<br>Municipality of Larissa<br>Roma Capitale |



| | |
|---|---|
| Document version: | 1.0 |

## Table of Contents

## Executive Summary

This deliverable of the CS-AWARE project is the second in an iterative series of three deliverables (D2.1 System and dependency analysis (first iteration) – Cybersecurity requirements for local public administrations, D2.2 System and dependency analysis (second iteration) - Pilot scenario definition and D2.3 System and dependency analysis (third iteration) – Pilot scenario specification and self-healing strategies) that will be delivered throughout the project run time. The second iteration picks up on the first iteration to refine our understanding in the three main thematic focus points covered in the original deliverable: an **initial threat assessment in the LPA context**, an **analysis of external information sources** and a **pilot specific analysis** in the partner municipalities of Larissa and Rome. In addition this deliverable adds a fourth focus point, the **definition of CS-AWARE use cases**, based on our understanding and results of the first three topics.

For the *initial threat analysis*, the updated versions of the reports covered in last year's deliverable were investigated for changes that would shift our understanding of risks in LPAs. It has shown that during the last year only minor shifts in the cybersecurity landscape could be observed, none of which were specifically relevant to our understanding of LPA risks. Based on those findings it was concluded that our initial risk analysis of D2.1 is still valid and does not need to be updated.

In the context of *analysis of external information sources*, D2.1 focused on classifying available information sources and identifying relevant sources in those classes. In D2.2 our focus shifted to those information sources that can be utilized for dynamic collection of cybersecurity relevant information specific to the CS-AWARE context. Based on the classification of D2.1, those sources are mainly related to threat intelligence, vulnerability data as well as social media sources. A challenge we saw specifically with threat intelligence sources was that there are a multitude of free and commercial data providers, yet little work has been done in assessing the quality of those providers. It was therefore decided to create a CS-AWARE specific scoring system to identify the most relevant information sources and shortlist those that should be collected with priority. This was done by defining a set of indicators, assigning an importance value to each indicator and assess all relevant sources based on those criteria. A shortlist of sources that will be considered with priority in CS-AWARE was created. Our results indicate that a methodical approach towards assessing the quality and relevance of information sources does offer some additional value to a purely intuitive selection. With respect to social media, it was already concluded in D2.1 that Twitter and Reddit will most likely provide the most relevant information for CS-AWARE, based on expected quality and accessibility of data. For D2.2 the challenge was to narrow the focus of data collection by identifying relevant users and communities in those two social media platforms that are considered relevant for cybersecurity and CS-AWARE. It was decided to use user/community based shortlisting since this usually yields in better results and less false positives as compared to keyword based shortlisting. Taking into account the dynamic nature of social networks, we see the list as a solid basis for the CS-AWARE data collection efforts that will dynamically evolve based on how the relevant users and communities evolve.

The *analysis of LPA specific information* was refined by the second round of system and dependency analysis workshops. After gaining a comprehensive overview of the core system setups by identifying the critical assets as well as dependencies among those assets during the first round of workshops (reported in D2.1), the challenge for deliverable 2.2 was to refine this understanding by identifying the critical processes of the services that are relevant for CS-AWARE piloting, and the associated information flows through the system and dependency graph that those processes create in day-to-day operations of both system users and administrators. To achieve this understanding, the workshops were organized in two parts: the system and dependency focused workshop to refine the understanding of systems and processes already started in the first round of workshops, as well as a more end-user focused story telling workshop to determine the cybersecurity related problems users and administrators alike face on a daily basis, and the

procedures and processes used to solve those problems. Based on the results of those workshops, as well as the initial risk analysis, the CS-AWARE team was able to define an approach to pilot scenario definition. It was concluded that the best approach will be to model the pilot scenarios after the information flows each relevant process creates in the systems. Monitoring and analysis will be mainly based on behavioural analysis of relevant information flows to detect unusual and suspicious behaviour. It was concluded that the monitoring points identified in D2.1 are able to capture the information required to perform this analysis.
In addition to the pilot scenarios, specific *use case scenarios* have been defined, based on the experience gained during the initial risk analysis, the analysis of data that is available from external information sources, as well as the requirements that end users and administrators have – derived from the results of the system and dependency analysis as well as storytelling workshops. Four specific use cases could be identified: Vulnerability awareness (map classified vulnerabilities to specific LPA systems/components), Behaviour analysis (identify suspicious behaviour and if possible classify according to data received from threat intelligence), General security warnings (inform about general and/or currently ongoing security events that may become relevant to the specific context of each LPA). The final use case, if the CS-AWARE project decides to allow analysis of some data considered personal identifiable data under GDPR rules (specifically IP and DNS entries), an analysis of connections originating from or going to specific IP/DNS entries that are classified as malicious by relevant communities can be conducted. While we assume that the list of use case scenarios covers all aspects relating to cybersecurity awareness that can be covered considering the data that is provided by the various communities, additional use cases may be added in case new information arrives.

# 1 Introduction

CS-AWARE Deliverable 2.*2 System and dependency analysis (second iteration) – Pilot scenario definition* continues the analysis started in Deliverable 2.1, provides an update as well as new work in the three core areas covered in the previous document: An initial threat assessment, an analysis of relevant external information sources, as well as an analysis of the CS-AWARE piloting scenarios. In addition, another Section was added in order to specify the CS-AWARE use case scenarios. Section 2 picks up on the initial threat analysis, revisits the initial conclusions and updates the view where necessary. Section 3 continues the work on identifying and analysing the relevant external information sources. While D2.1 was mainly focused on identifying the classes of information that are available in general and collecting available information sources related to those classes, D2.2 is concerned with identifying the most relevant information sources for the CS-AWARE context. Section 4 continues the analysis of the pilot partner systems in the Municipalities of Larissa and Rome, by detailing the results of the second round of soft systems workshops. In addition to the system and dependency focused workshop sessions, end-user focused story telling workshop sessions were introduced to capture also the end-user perspective relating to cybersecurity in their day-to-day work in the Municipalities. Looking at those aspects allowed to define the approach taken towards pilot scenario definition in Section 4.5. It should be noted that the details relating to the pilot scenarios are part of the non-public Annex 9 of this document, due to the confidential nature of this information and the related potential security concerns associated with disclosing this information. Section 5 concludes this deliverable by defining the use case scenarios taken into account in the CS-AWARE context, based on our understanding of the available information from external information sources as well as the requirements that end users as well as administrators have voiced during the workshops in the municipalities.
Annex 1 details the results of the quantitative analysis performed on external information sources, Annex 2 contains the introductory presentation to SSM given in the end user workshops, and finally

Annex 3, Annex 4, Annex 5, Annex 6, Annex 7 and Annex 8 contain the results of the end user workshops in the Municipalities of Larissa and Rome.

# 2 Initial Threat Assessment

In this Section we revisit the initial threat assessment of CS-AWARE Deliverable 2.1, which was submitted only a few months after the project started. For this purpose we monitored the threat landscape over the past year and studied the updated versions of the key reports in this area, most notably the ENISA threat landscape of 2017 (ENISA, 2017) and the Europol Internet Organized Crime Threat Assessment of 2018 (Europol, 2018). As can be seen in Figure 1, the top 15 threats remained the same between 2016 and 2017, only the ranking and volume changed. We conclude that for the context of CS-AWARE no relevant changes happened during this time period.

| Top Threats 2016 | Assessed Trends 2016 | Top Threats 2017 | Assessed Trends 2017 | Change in ranking |
|---|---|---|---|---|
| 1. Malware | ↑ | 1. Malware | → | → |
| 2. Web based attacks | ↑ | 2. Web based attacks | ↑ | → |
| 3. Web application attacks | ↑ | 3. Web application attacks | ↑ | → |
| 4. Denial of service | ↑ | 4. Phishing | ↑ | ↑ |
| 5. Botnets | ↑ | 5. Spam | ↑ | ↑ |
| 6. Phishing | → | 6. Denial of service | ↑ | ↓ |
| 7. Spam | ↓ | 7. Ransomware | ↑ | ↑ |
| 8. Ransomware | → | 8. Botnets | ↑ | ↓ |
| 9. Insider threat | → | 9. Insider threat | → | → |
| 10. Physical manipulation/damage/ theft/loss | ↑ | 10. Physical manipulation/damage/ theft/loss | → | → |
| 11. Exploit kits | ↑ | 11. Data breaches | ↑ | ↑ |
| 12. Data breaches | ↑ | 12. Identity theft | ↑ | ↑ |
| 13. Identity theft | ↓ | 13. Information leakage | ↑ | ↑ |
| 14. Information leakage | ↑ | 14. Exploit kits | ↓ | ↓ |
| 15. Cyber espionage | ↓ | 15. Cyber espionage | ↑ | → |

Legend: Trends: ↓ Declining, → Stable, ↑ Increasing
Ranking: ↑ Going up, → Same, ↓ Going down

*Figure 1: ENISA Threat assessment comparison 2016/2017*

Similar conclusions can be drawn from the IOCTA report, which sees a stable threat landscape when observed from the law enforcement perspective. Notably the IOCTA report stresses the increasing relevance of collaboration and cooperation in cybersecurity, an assessment that we share in the CS-AWARE project. Most relevant for CS-AWARE is that the report emphasises on the close relation of data breaches and network attacks (illegally acquiring, destroying or denying

access to data after breaching systems via network attacks), an assessment that we share based on our experiences and CS-AWARE end user workshops.
In conclusion we assess that our initial threat assessment of Deliverable 2.1 is still valid, with the core statement that the data managed by LPAs is the most valuable asset to protect, and all threats against that data are to be considered relevant. The details related to this initial threat assessment can be found in Deliverable 2.1.

# 3 Analysis of External Information Sources

CS-AWARE Deliverable 2.1 was focused on generally identifying possible external information sources to be used for CS-AWARE that can help in analysing LPA cybersecurity incidents and help raise cybersecurity awareness. For deliverable 2.2 the main task is to find a way to assess the relevance and quality of those sources (and additional sources that have emerged over the past year), and to create a short-list of sources that are relevant for the CS-AWARE continuous data collection and analysis. From the 9 general classes of information sources that have been identified and are listed in Daeliverable 2.1, the following classes have been excluded from further analysis:

- **Malware analysis:** CS-AWARE focuses on analysis of metadata rather than conducting deep inspection of files or network packets which would be required to utilize most of the relevant data that can be retrieved from malware analysis focused information sources.
- **Cybersecurity visualizations:** Those information sources may be relevant for finding approaches to visualize CS-AWARE findings, but do not need to be further analysed in the context of continuous data collection.
- **Other information sources:** The sources listed there are either not relevant or are implicit to other sources.

This Section will start (Section 3.1) with a definition of CS-AWARE quality indicators defined to determine the quality of

1. **NIS competent authorities** (a combination of NIS competent authorities and law enforcement agencies as listed in deliverable 2.1)
2. **Threat intelligence platforms** (a combination of relevant sources from deliverable 2.1 cyber intelligence sources and information sharing tools, cyber intelligence data feeds and vulnerability data)

The results of the analysis are shown in Section 3.2. Section 3.3 lists our results for shortlisting and defining relevant data to collect from **social media** sources, which required a different analysis approach.

## 3.1 Definition of Quality Indicators for NIS competent authorities and threat intelligence platforms

After the initial analysis of external information sources in Deliverable 2.1 it became apparent that especially in the field of threat intelligence, there are many providers active and that a shortlist of high quality information sources applicable to the CS-AWARE context is necessary, since the body of knowledge that is shared by the different providers is not expected to differ to such an extent that collection from all sources is required. Analysis of related work has shown that only limited work has been done in providing a reliable scoring system, ideally based on quantitative criteria, and that there is no readily available metric or scoring system available that would suit our needs. An interesting approach is presented in (Meier, Scherrer, Gugelmann, Lenders, & Vanbever, 2018),

where a ranking algorithm similar to Googles page rank is proposed to assess cyber threat intelligence feeds based on the criteria "completeness of information", "accuracy of information" and "speed". However, to the best of our knowledge, such a system is not yet available for public use. Another interesting approach is presented in (Hanson, 2015) where the admiralty code ("Validity of Claim", "Reliability of Source") is used in an automated system to evaluate information. Again, to the best of our knowledge such an approach has not been applied to assess the quality of threat intelligence and we can thus not rely on such results. Most other relevant related work is concerned with qualitative indicators applicable to specific contexts, none of which fulfilled the requirements of CS-AWARE.

Based on the findings in related work, and the fact that there are no readily available metrics or scoring systems for our context, it was decided to define a set of indicators/metrics to assess, on a qualitative level, the quality of the relevant information sources. It was decided to assess the NIS competent authorities and the threat intelligence platforms based on the same set of indicators, but assess their relevance separately. We identified 6 main indicators, each split into sub-categories, which are described in detail in Table 1.

*Table 1: CS-AWARE Quality Indicators for information sources*

| Indicator | Explanation |
|---|---|
| **1 Quality of Data** | **An indicator to assess the expected quality of data from an information source. It was decided to assess the quality based on the complexity of information that is shared by a source, according to state-of-the-art threat intelligence concepts.** |
| 1.1 Indicators | An indicator is a collection of cyber security relevant information containing patterns that can be used to detect suspicious or malicious cyber activity. |
| 1.2 Sightings | A sighting is an observation that someone has shared with the community, without adding additional intelligence to it. |
| 1.3 Courses of Action | A course of action is information concerning how to prevent or mitigate an event shared by e.g. an indicator. |
| 1.4 Vulnerabilities | A vulnerability is a weakness in a hardware or software appliance that could be exploited to breach the appliance. |
| **2 Provider Classification** | **An indicator to assess the type of sharing an information sharing provider does, and how much original information can be expected from this provider.** |
| 2.1 Data Feed Provider | A data feed provider is the entity that produces cyber security information, or shares received information with minimal or no additional intelligence added to it. |
| 2.1.1 Provides Original Data | A data feed provider that is the original provider of this information, which has been shared in one form or another by the source of e.g. an incident. |
| 2.1.2 Provides Aggregated Data | A feed provider that aggregates data originating from various sources. |
| 2.2 Intelligence Platform | A provider that adds intelligence/ analysis to the information that is shared with the provider in one form or another. |
| 2.3 Report Provider | A provider that provides e.g. statistical information in form of reports rather than data feeds. |
| **3 Licencing Options** | **An indicator to assess the licencing of data use and/or access to the data source API.** |
| 3.1 Open (Publicly available) | The data is freely available to collect and use. |
| 3.2 Restricted use | Some restrictions apply as to how the data can be used (e.g. academic or commercial context). |
| 3.3 Commercial | The data provider has commercial interest and provides the data |

| | |
|---|---|
| | for a fee. |
| 3.4 Information Reuse | Specifies how the data provided by a data source can be reused. Options include commercial, academic or personal use. |
| 3.4.1 Commercial use allowed | The data can be reused in a commercial context, it is allowed to offer services and collect fees for services based on this data. |
| 3.4.2 Academic use allowed | The data can be used in an academic context without restrictions, restrictions apply in other contexts.. |
| 3.4.3 Personal use allowed | The data can be used for personal use without restrictions, restrictions apply for other contexts. |
| **4 Interoperability/Standards** | **An indicator to assess the interoperability of a tool provider with state-of-the art cybersecurity threat exchange standards and relevant tools/libraries.** |
| 4.1 STIX1 | Supports the STIX1 threat expression standard. |
| 4.2 STIX2 | Supports the STIX2 threat expression standard. |
| 2.3 TAXII | Supports the TAXII threat exchange protocol standard. |
| 4.4 OpenIOC | Supports the OpenIOC cybersecurity artefact description standard. |
| 4.5 RSS | Supports the RSS feed standard. |
| 4.6 JSON | Supports the JSON protocol data exchange format. |
| 4.7 CSV | Supports the CSV data expression standard. |
| 4.8 Plain Text | Supports plain text data expression. |
| **5 Advanced API** | **An indicator to assess if a data source supports or enables relevant advanced API features.** |
| 5.1 Filtering based on time | Supports filtering based on time for data access. Relevant for data collection to only collect entries since last access. |
| 5.2 Filtering based on content | Supports filtering based on content. Relevant for context specific data collection. |
| **6 Context applicable content** | **An indicator to assess if a data source provides data that is in general relevant to the CS-AWARE context.** |
| 6.1 Vulnerabilities | The data source provides information about vulnerabilities. |
| 6.2 Threats | The data source provides information about threats. |
| 6.3 Campaigns | The data source provides advanced intelligence about cybersecurity campaigns. |
| 6.4 Hashes | The data source provides cybersecurity relevant hashes (e.g. malware hashes) |
| 6.5 Recommendations | The information source provides general cybersecurity recommendations. |
| 6.6 Incidents (Sightings) | The information source provides observed incidents or sightings without advanced intelligence. |

The resulting analysis of threat intelligence sources based on those indicators can be found in Annex 1 of this document.

## 3.2 Shortlist of relevant cybersecurity intelligence information sources

In this Section we show the results of our shortlisting efforts based on applying an importance value to each of the indicators found in Table 1 and thus assigning a score to each source identified and classified in Annex 1. This scoring was done individually for the list of NIS competent authorities and threat intelligence sources. The final list almost exclusively contains pure cybersecurity intelligence information sources, since it was concluded that while NIS competent authorities provide excellent data for the more static analysis, the dynamic information provided by those sources are most likely also covered by threat intelligence sources which have the advantage of

better interoperability and support of information collection standards. It should be noted that the CS-AWARE project reserves the right to remove or add information sources should new information arrive, but we see this list as a basis for our data collection and analysis considerations.
For the threat intelligence sources we applied the scoring schema found in Table 2. Scores **of 5 are seen as the highest priority** for CS-AWARE, while scores of **1 are seen as the lowest priority** for CS-AWARE. An indicative reasoning why we assigned those importance values is given in the table. For completeness it should be noted that, when applying the scoring of Table 2 to the NIS competent authorities list found in Annex 1, those sources that also provide some kind of data feed (CERT-EU, national CERT examples) scored the highest, followed by those sources that provide mainly reports (Enisa, Europol, Interpol). Since it was already concluded above that NIS competent authorities are less relevant for dynamic data collection, we consider those results irrelevant for our goal of shortlisting CS-AWARE relevant dynamic information sources. The scoring applied to the threat intelligence platforms listed in Annex 1 can be found in Table 3. In this case meaningful results were produced in our effort of shortlisting the information sources, and in many cases confirmed the analysts' intuition of what should be the most relevant threat intelligence sources for our context. In some cases, however, like for example the US-CERT AIS, the analysts had not expected such a high score which shows that a methodical approach towards selection of relevant sources is indeed required. CERT-US AIS provides, unlike the European counterpart CERT-EU, a sophisticated cyber intelligence information feed. In Europe such initiatives exist as well, like for example the MISP platform which is found on our shortlist, but those initiatives are not directly associated with the European CERT.
We think that at this point this list gives us a solid basis for information collection covering all CS-AWARE use cases as described in Section 5 of this document, the scoring also gives us the possibility to identify additional quality sources further down the list in case it is discovered that specific relevant information is not covered yet by the sources that scored the highest according to our method.

*Table 2: Scoring table for CS-AWARE threat intelligence source quality indicators*

| | 1 | 2 | 3 | 4 | 5 |
|---|---|---|---|---|---|
| **1. Quality** | Regarding the expected quality of data, the most relevant aspects for CS-AWARE will be indicators, vulnerabilities and courses of actions. Simple sightings are important, but seen less relevant to the expected quality in the CS-AWARE context. | | | | |
| 1.1 Indicators | | | | | + |
| 1.2 Sightings | | | + | | |
| 1.3 Courses of Action | | | | + | |
| 1.4 Vulnerabilities | | | | | + |
| **2. Provider Classification** | In the CS-AWARE context, platforms that add intelligence to cybersecurity related data are seen as the highest priority. Data feed providers are important, but have lower priority. At this point we do not distinguish if a data feed provider is an original data provider or an aggregator. | | | | |
| 2.1 Data feed provider | | | + | | |
| 2.1.1 Original Provider | | | + | | |
| 2.1.2 Aggregator | | | + | | |
| 2.2 Intelligence Platform | | | | | + |

| | | | | | |
|---|---|---|---|---|---|
| 2.3 Report Provider | + | | | | |
| **3. Licensing Options** | Regarding the licensing options, openly available data has the highest priority, whereas restricted use and commercial options are of lower priority. Regarding information reuse, we see those that allow commercial reuse as having the highest priority, while those sources allowing only personal use have the lowest priority. | | | | |
| 3.1 Open (publicly available) | | | | | + |
| 3.2 Restricted | | | + | | |
| 3.3 Commercial | + | | | | |
| *3.4 Information Reuse* | | | | | |
| 3.4.1 Commercial: Allowed | | | | | + |
| 3.4.2 Academic: Allowed | | | + | | |
| 3.4.3 Personal: Allowed | + | | | | |
| **4. Interoperability** | For CS-AWARE we prioritize those sources that are compatible with the relevant cybersecurity specific data exchange formats. More general formats are relevant, but classified with lower priority. | | | | |
| *4.1 Supported standards (data formats)* | | | | | |
| 4.1.1 STIX1 | | | | | + |
| 4.1.2 STIX2 | | | | | + |
| 4.1.3 TAXII | | | | | + |
| 4.1.4 OpenIOC | | | | | + |
| 4.1.5 RSS | | | + | | |
| 4.1.6 JSON | | | | | + |
| 4.1.7 CSV | | | | + | |
| 4.1.8 Plain Text | | + | | | |
| **5. Advanced API Supported** | Advanced API support is a nice to have feature, but is generally not classified with the highest priority in the CS-AWARE context. | | | | |
| 5.1 Filtering based on dates | | | + | | |
| 5.2 Filtering based on types of information e.g. vulnerabilities only, threats, campaigns | | + | | | |
| **6. Source applicable to our context** | Based on the use cases that have been discussed for the CS-AWARE context and will be explicitly specified in Section 5 of this document, vulnerabilities and threats have been classified with the highest priority. Sources that also provide modelling of more advanced campaigns or that provide recommendations as to how to mitigate cybersecurity incidents are seen to be of relevance as well. | | | | |
| 6.1 Vulnerabilities | | | | | + |
| 6.2 Threats | | | | | + |
| 6.3 Campaigns | | | + | | |

| | | | | | |
|---|---|---|---|---|---|
| 6.4 Hashes | + | | | | |
| 6.5 Recommendations | | | | + | |
| 6.6 Incidents (Sightings) | | | + | | |

*Table 3: Threat intelligence sources shortlist*

| Position | Source Name | Source URL |
|---|---|---|
| 1 | MISP Platform | http://www.misp-project.org/index.html |
| 2 | Anomali Staxx | https://www.anomali.com/community/staxx |
| 3 | HailATaxii | http://hailataxii.com |
| 4 | Soltra Edge | https://soltra.com/en/ |
| 5 | US-CERT AIS | https://www.us-cert.gov/ais |
| 6 | CVEDetails | https://www.cvedetails.com/ |
| 7 | Abuse.ch | https://abuse.ch/ |
| 8 | OTX Ailienvault | https://otx.alienvault.com/ |
| 9 | Blocklist | http://www.blocklist.de |
| 10 | Nist NVD | https://nvd.nist.gov/ |
| 11 | Collaborative Research into Threat (CRiT) | https://github.com/crits/crits |

## 3.3 Shortlist of relevant social media sources

Shortlisting the relevant social media information sources was simple, since it was already concluded in Deliverable 2.1 that Reddit and Twitter are the two most relevant social media information sources for CS-AWARE based on accessibility, licencing and expected quality if information. A more detailed reasoning can be found in Deliverable 2.1. Instead of identifying relevant indicators/metrics for shortlisting of sources, the challenge with respect to social media was to identify and short-list the relevant users or topic groups that provide high quality information. It was decided to refrain from using keywords based searches, to avoid the data pollution to be expected by searching for broad keywords. User-based shortlisting promises better results since trusted user/ cybersecurity experts or topically focused communities can be chosen. The process of how to identify those users/communities was roughly the following:

- Identify discussions (blogs, forums, social media posts, …) that were reasoning about the most relevant social media sources for security
- Cross-check those discussions to identify the most relevant subset of users/communities to collect information from
- Perform a qualitative analysis of those users/communities to 1) check if they exist, 2) check if they provide relevant information and 3) check if the quality of information seems to indicate a quality source

Table 1 lists the relevant users/communities that were identified. It should be noted that the CS-AWARE project reserves the right to add/remove entries from this list, should new information arise. However, we will use this list as a basis for information collection and analysis with respect to social media. It is generally expected that this list will grow over the project life time.

*Table 4: Relevant users/communities from identified sociel media sources*

| Social media source/ Relevant User/Community |
|---|
| **Reddit** |

| |
|---|
| https://www.reddit.com/r/antiforensics |
| https://www.reddit.com/r/crypto |
| https://www.reddit.com/r/cyberlaws |
| https://www.reddit.com/r/malware |
| https://www.reddit.com/r/ReverseEngineering |
| https://www.reddit.com/r/netsec |
| https://www.reddit.com/r/blackhat |
| https://www.reddit.com/r/computerforensics |
| https://www.reddit.com/r/netsecstudents |
| https://www.reddit.com/r/pwned |
| https://www.reddit.com/r/AskNetsec |
| https://www.reddit.com/r/cybersecurity |
| https://www.reddit.com/r/Information_Security |
| https://www.reddit.com/r/ISO27001/ |
| https://www.reddit.com/r/infosecurity |
| https://www.reddit.com/r/websecurity |
| https://www.reddit.com/r/fulldisclosure |
| https://www.reddit.com/r/security |
| https://www.reddit.com/r/compsec |
| https://www.reddit.com/r/bugbounty |
| https://www.reddit.com/r/masterhacker |
| https://www.reddit.com/r/Cybercrime |
| https://www.reddit.com/r/cyb3rs3c |
| **Twitter** |
| @briankrebs, @Dejan_Kosutic, @msftsecresponse, @PrivacyProf, @runasand, @gattaca, @selenakyle @dangoodin001, @infosecEditor, @gcluley, @SwiftOnSecurity, @EFF, @samykamkar, @thegrugq, @FRSecure, @InfoSecInstitute, @Symantec, @InfosecurityMag, @Rivetz, @IBMSecurity, @k8em0, @PolySwarm, @HaveIBeenPwned, @SwiftonSecurity, @Troyhunt, @e_kaspersky, @StewartRoom, @mikko, @joshcorman, @lutasecurity, @BrianHonan, @annie_bdc, @taosecurity, @jeremiahg, @schneierblog, @neiljrubenking, @dangoodin001, @gcluley, @campuscodi, @peterkruse, @Shirastweet, @nakashimae, @iblametom, @evacide, @DanielMiessler, @evanderburg, @ScottBVS, @jack_daniel, @anton_chuvakin, @lennyzeltser, @josephsteinberg, @RobertMLee, @runasand, @TroelsOerting, @ejhilbert, @PatrickCMiller, @peterwsinger, @Shadowserver, @sans_isc , @EC3Europol, @IntelSecurity, @enisa_eu, @CERTEU, @abuse_ch, @spamhaus, @Eurosint, @Anomali, @AbuseIO, @GlobalCyberAlln, @MISPProject, @CyberIntelFeed, @pulsedive, @malware_traffic, @InfosecurityMag, @USCERT_gov |

# 4 Analysis of Pilot Scenarios and LPA Specific Information Sources

In this Section the pilot scenario definition for the two LPA pilots of CS-AWARE in the Municipalities of Larissa and Rome will be described, following up on the analysis results from the first round of end user workshops described in Deliverable 2.1.

The Section starts by detailing the results of the second round of end user workshops in the Municipalities of Larissa and Rome (Sections 4.2 and 4.3). In both cases the workshop started with a refinement of the asset and dependency graph that derived from the rich pictures produced during the first round of soft systems analysis, based on

1) A better understanding of the business processes that are made available to the municipalities by the critical services previously identified
2) A refinement of the asset and dependency graph by revisiting it together with the workshop participants
3) A mapping of the information flows each business process produces in the system and dependency graph

An important tool to achieve the first point was a business process analysis according to CATWOE analysis, which is part of Step 3 of the SSM methodology. CATWOE is a mnemonic and is a tool for identifying the Customers, Actors Transformations, World view Owners, and Environmental constraints that are depicted in a Rich Picture. In this second workshop, the analysts wanted to closely examine the Transformations evident in the Rich Pictures as these enabled the analysts to develop a detailed understanding of the underlying processes of Larissa's and Rome's systems and networks. Furthermore, the identification of Customers and Actors allowed them to better determine the interactions with those systems.
The second part of each workshop was focused on bringing an additional element into the understanding of the operations of the municipalities, as well as how this interacts with our understanding of the systems and dependencies: The perspective of the system end users based on stories of cybersecurity and how it is perceived by the end users based on storytelling workshops. Since this is a new perspective and methodology in CS-AWARE that was not part of the first round of workshops or Deliverable 2.1, the concept will be explained in more detail in Section 4.1. The conclusions drawn from the user workshops in Larissa and Rome are presented in Section 4.4.
In Section 4.5, we will show how possible pilot scenarios can be derived from the information gained during the workshops. It should be noted that the actual asset and dependency graphs, as well as the pilot scenarios are in a non-public Annex (Annex 9) of this deliverable due to confidentiality and the potential security implications of making this information public. It should also be noted that in all parts of the workshops the participants have been asked to visualize the information on flip boards (e.g. CATWOE, user stories). Records in the form of photographs have been kept of all relevant flip board sheets, but the authors of the deliverables have decided to reproduce the information in textual form for better readability of the document. The photographs of the original flip board sheets are however available to the CS-AWARE project, if required.

## 4.1 Introduction to storytelling workshops in the context of cybersecurity

In October and November 2018, the CS-AWARE project organised one-day workshops in the context of the second round of end user workshops that were held at the premises of the municipalities that participated in the project. Participants in these workshops were system administrators and users of the services provided by the system, in other words, members of the organisation we call municipality. These workshops followed the second series of soft systems analysis workshops, during which the system administrators went more deeply into the complexities of the municipality system network. This Section discusses the one-day workshop, that we call *the story-telling workshop*.
The purpose of this activity was for the CS-AWARE project to develop greater understanding and more awareness of the experiences of the users and the system administrators in relation to cybersecurity issues. We wanted to obtain a sketch of actual and hypothetical cases of cybersecurity dangers, and the needs, roles and issues of people dealing with these dangers in their professional contexts. This is a necessary asset for our project, because no technology solution can be successful without considering user needs, in addition to involving the users in the design of the technology.
We decided that the best way to capture experiences was in the form of a story. The story telling workshop involved small groups of participants from the municipality (system administrators and users from various departments) in collaborative efforts to produce meaningful stories about their

cybersecurity experiences. These stories were presented and verified with all participants, including members of the CS-AWARE project. The stories are reported and analysed in a theoretical framework that aims to capture stories about how organisations deal with cybersecurity issues.
The first story-telling workshop was organised in the Municipality of Larissa, on Thursday October 4th, referred to as Workshop I. This report will be combined with the report from the Municipality of Roma Capitale, where a similar workshop (Workshop II) took place on November 22nd.
The workshops are generally based on concepts of (Kurtz, 2012) and (Snowden, 2005), in order to capture user perspectives and awareness. Figure 2 shows that we start with a recollection of some individual experiences related to cybersecurity (upper triangle). These experiences are subsequently further elaborated in small groups, a process we call *broadening and deepening* (Baker, Andriessen, Lund, Amelsvoort, & Quignard).Topics in the story are broadened by adding more topics (e.g. the role of the organisation, the role of the system, the actions of the protagonist), and each topic can be deepened by going further along the path of perspectives, actions and feelings that characterise a topic. This broadening and deepening is done in small collaborative groups. Collaborative groups can help with reflection and elaboration, add multiple perspectives, and generally may enhance the range and depth of an experience into a story (Stahl, 2013). Our view of stories does not focus on creating narratives, but we aim for a set of coherent elements that characterise some event, within a context (orientation), the issue (the complication) and the outcome (the resolution).

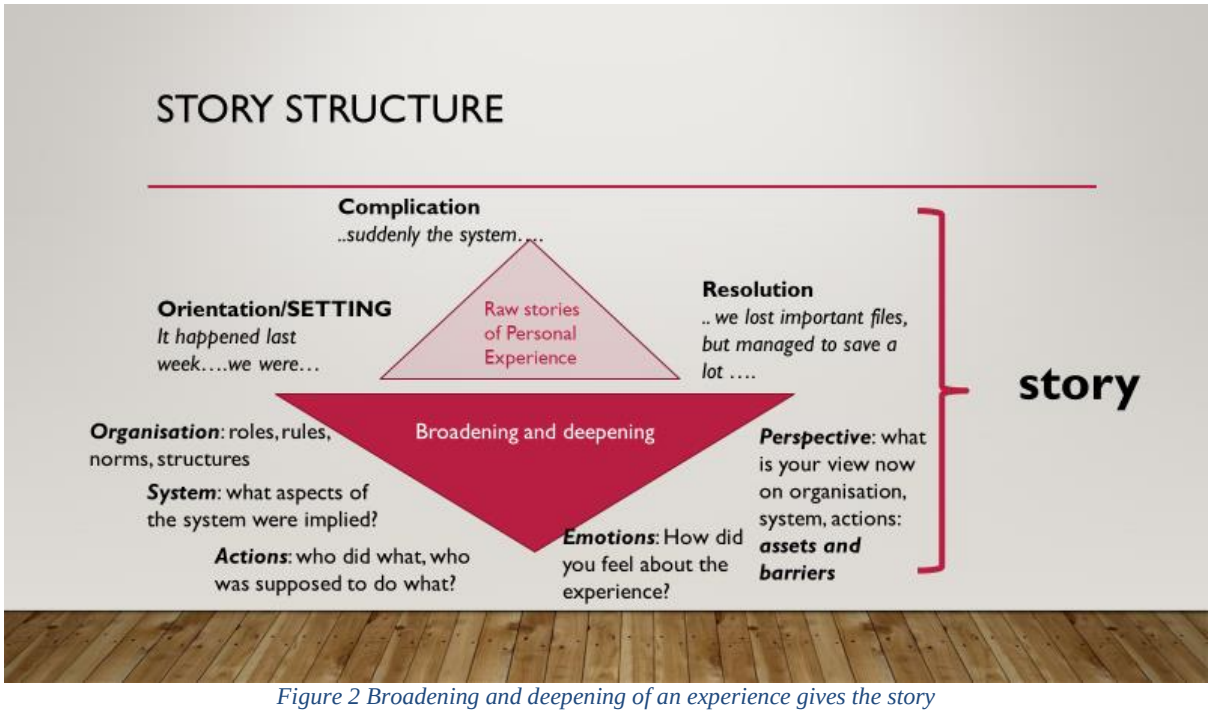



*Figure 2 Broadening and deepening of an experience gives the story*

Our analysis takes as a starting point the view of the user in his organisation, not the nature of the technological issue. Therefore, we need a framework that does justice to the organisation in which the user is working, and how that relates to how a user experiences the technological issues, including their resolution. We consider this user with an issue as an activity system.
Activity theory begins with the notion of activity. An activity is seen as a system of human "doing" whereby a subject works on an object in order to obtain a desired outcome. In Figure 3 below "the object is depicted with the help of an oval indicating that object-oriented actions are always, explicitly or implicitly, characterized by ambiguity, surprise, interpretation, sense making, and potential for change" (Engeström, Expansive Learning at Work: Toward an activity theoretical reconceptualization., 2001). In order to do this, the subject employs tools, which may be external

(e.g. an axe, a computer) or internal (e.g. a plan). As an illustration, an activity might be the operation of an automated call centre. Many subjects may be involved in the activity and each subject may have one or more motives (e.g. improved supply management, career advancement or gaining control over a vital organisational power source). A simple example of an activity within a call centre might be a telephone operator (subject) who is modifying a customer's billing record (object) so that the billing data is correct (outcome) using a graphical front end to a database (tool). An activity is a hierarchical structure, and its nature changes over time (Leont'ev, 1974). This change can be related to tensions in the system, so tensions can be a good thing.

For our purposes it is important to consider the tool, which 'mediates' between the activity and the object. "The tool is at the same time both enabling and limiting: it empowers the subject in the transformation process with the historically collected experience and skill 'crystallised' to it, but it also restricts the interaction to be from the perspective of that particular tool or instrument; other potential features of an object remain invisible to the subject..." (Foot, 2001).

An activity system further pictures an individual as part of a system characterised by particular rules, communities and division of labour (Engeström, Miettinen, & Punamäki, Perspectives on Activity Theory, 1999). All activity is carried out within a social context, more specifically in a community of people. The way in which the activity is situated in this context can be characterised by rules, which formally or informally mediate between subjects and a community, and by a division of labour, mediating between objects and the community.

Activity theorists argue that consciousness is not a set of discrete disembodied cognitive acts (decision making, classification, remembering), and certainly it is not the brain; rather, consciousness is located in everyday practice: “you are what you do." (Nardi, 1996). (Nardi, 1996) also argued that "activity theory proposes a strong notion of mediation—all human experience is shaped by the tools and sign systems we use."

For the analysis and description of the overall picture emerging from these stories we envisage two activity systems, one of the (internal/municipality) users, and other one of the IT-Department.

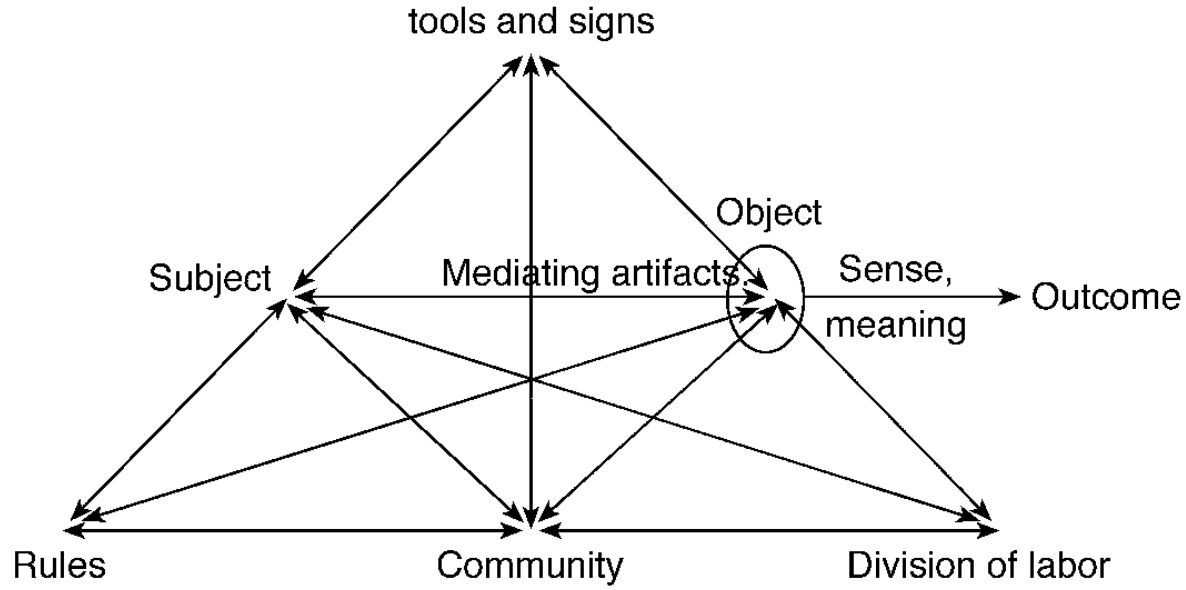



*Figure 3:* The structure of a human activity system *(Engeström, Learning by Expanding: an activity-theoretical approach to developmental research, 1987)*

In the context of D2.2 we are mainly concerned about how the results of the user story workshops will influence our understanding of the asset and dependency graph; the processes, interactions and transformations of data based on this graph and how the users (actors and customers) of the system influence this in order to be able to define relevant pilot scenarios. It should be noted however that

the process started in the story telling workshops will also be an important aspect in preparation for the piloting phase in work package 5, and are relevant in preparation for Deliverables 5.1, 5.2 and 5.3.

**All workshops and the reports based on them, respect the privacy of thier participants. Therefore D7.1 (Information Sheet and Consent Form) was given to all participants before the start of the workshop, participants were asked to sign that they consent to their participation in the workshop. The report is sent to participants for verification. There are no video recordings made, some parts are recorded on audio, solely for the purpose of analysis, with full consent of the participants.**

## 4.2 Second Soft Systems Workshop in the Municipality of Larissa (1.10 - 5.10.2018)

The second workshop in Larissa commenced on October 1st 2018. The workshop ran for three days and was followed by the story telling workshop part. The visiting project team of analyst / facilitators comprised as follows:

| Organization | Participant |
|---|---|
| University of Oulu | Christian Wieser |
| University of Vienna | Thomas Schaberreiter<br>Veronika Kupfersberger |
| CARIS Research Ltd | Christopher Wills |
| Wise&Munro | Jerry Andriessen |
| OTS | George Apostolopoulos |
| Municipality of Larissa | Christos Topalidis<br>Heleni Drakou<br>Georgia Kolovou<br>Antigoni Mezari<br>Thanasis Poultsidis |

In addition, for the story telling workshop part several end users of the identified key systems (all employees of the Municipality of Larissa) were present, but since they are not part of the core CS-AWARE team, their names are not made public in this document for data protection reasons.
Section 4.2.1 will detail the system and dependency analysis focused workshop part, and Section 4.2.2 will detail the end user focused story telling workshop including the respective main results of each workshop part.

### 4.2.1 Part 1: System and dependency analysis

Prior to the workshop, the key systems that were identified during the first workshop were translated into a high level GraphingWiki graph before the second workshop, representing the key assets and dependencies relevant for CS-AWARE. These key systems were represented in the following Rich Pictures, which can be found in Annex 2 of CS-AWARE deliverable 2.1. The high level graph can be found in the non-public Annex 9.

- Day 1 RP1
- Day 1 RP 4
- Day 1 RP 7
- Day 2 RP 1
- Day 2 RP 4
- Day 2 RP 7

The workshop began with a presentation by Chris Wills on Root Definitions and Conceptual Models. This presentation can be found in Annex 2. The Larissa team reconfirmed that the Genesis and HRMS services contained the key processes in the municipality's operations.
Having obtained a good understanding of Larissa's network topography from the first workshop, one of the analysts' key tasks in this second workshop was to develop an understanding of the underlying processes of the City's operations. Agreement emerged that this could best be facilitated by using the CATWOE tool directly to explore the City's processes, rather than first using the intermediate SSM stage of developing Root Definitions.
The processes involved are described in the "Transformation" stage of CATWOE. The system called Genesis was identified as being a key mission critical system in Larissa. It is comprised of six subsystems:

1. Finance - Expenses
2. Finance – Revenues
3. Document Archiving
4. Web services – statistics for the Ministry of Finance
5. Permits – to open businesses, shops etc.
6. Decisions of City Council and its committees

Each of these subsystems were examined using CATWOE, the results can be found in Annex 3. The systems called HRMS (Human Resources Management System) comprise three sub systems:

1. Payroll management
2. HR management
3. Leave management

All three handle personal data and are therefore mission critical systems. All handle some aspects related to the payment of employees and are therefore mission critical. The results of the CATWOE analysis of each process can be found in Annex 4. Achieve the results of CATWOE analysis took around 1.5 days, and it allowed us to gain insight in the day-to-day operations of HRMS and GENESIS, and most importantly which data is handled, by who this data is handled and what are the transformations the data goes though during those operations. Those are important results relevant for the later stages of the workshop.
The remainder of the second day was utilized to review the findings of the first workshop, and to refine the transformation of those findings to a GraphingWiki asset and dependency graph. During this process the analysts guided the participants through the elements of the graph, facilitating discussion with the operators and users of the systems as to whether those elements were in the correct place and whether all of the relevant elements had been considered. This process was productive; many inaccuracies and incorrect elements could be identified, following up on the results from the previous workshops modelled in a structured and holistic way. Additionally, since the results were mapped in an intuitively understandable graph, relevant additions to the model could be made that had not been considered in previous sessions. The original graph, as well as the refined graph, together with an explanation of the chosen modelling approach can be found in the non-public Annex 9 of this deliverable. It was decided that due to the sensitivity of the results and possible security implications that the results should not be made public.
The third day of the workshop was concerned with trying to understand how the information flows through the systems during day-to-day operations of the critical systems. This analysis was done by mapping the results of the CATWOE analysis for each relevant business process to the asset and dependency graph modelled in GraphingWiki. Knowing the critical information flows and

transformations in the systems facilitates the analysts to focus on the monitoring and analysis requirements, in order to be able to define meaningful pilot scenarios for CS-AWARE. The identification of actors and customers for each process enabled the analysts to identify the entry and exit points of data to the Municipalities systems, and the identification of transformations enabled the identification of the relevant components and sub-systems involved in the transformation. The results of this analysis can be found in the non-public Annex 9 of this deliverable. The final step was to review the monitoring points that had been identified in the previous workshops, the result of which can be found in the non-public Annex 9. It was concluded that the previously identified monitoring points are indeed those that will provide the required information – no monitoring points were added or removed.
After the analyst team was satisfied that they had achieved the required level of detail to be able to define the pilot scenarios from a system and dependency analysis perspective, the system and dependency analysis part of the workshop was concluded and the participants were asked to reconvene the next day for the story telling part of the workshop.

#### *4.2.1.1 Workshop Discussion and Results*

The outcome of the second workshop in Larissa was that the analysts gained a clear understanding of Larissa's networks, systems, processes and information flows. This understanding was underwritten and confirmed by the Larissa personnel who participated in the workshops. The analysts were able to identify the key systems and processes in Larissa (those that either stored, processed data that was mission-critical to Larissa[1] or stored or processed sensitive or personal information[2]). The analysts were able to identify the most appropriate locations in Larissa's networks and systems where data could be monitored without compromising the privacy of citizens in breach of the GDPR, based on an identification of the information flows for the processes of the key systems.

### 4.2.2 Part 2: End user focused sessions

Present at Workshop I were four system administrators who had also participated during the three previous days in the SDA workshop. The local team leader had engaged 10 additional public administrators, from several departments of the organisation. Four researchers from the CS-AWARE project also took part, as moderators. Initially, all participants were divided in four groups of 3-5 members each. As the meeting evolved, some people left and a few others arrived, and the original groups mingled into different compositions. Three weeks before the workshop we asked the participants by email to send us short stories of cybersecurity experiences. With this preparatory assignment, we hoped to focus the awareness process on an individual level in order to give participants space for their own ideas. We received eight stories that guided our expectations of topics for the stories.
The story telling workshop started with a brief introduction of the CS-AWARE project by Thomas Schaberreiter and an explanatory talk by Jerry Andriessen about the general workshop concepts and procedures. All participants from the municipality were (again) asked to individually generate an experience that involved some issue with the cybersecurity of their organisation. It was free for them to write it down or not. After ten minutes participants were asked to join their group. The task of the group was to develop the story by adding topics to the experience and to provide these topics with more depth. The groups could discuss in their native language, but they were asked to put the

[1] Mission-critical in that it would either undermine the finances of the municipality or negatively impact the ability of the municipality to deliver key services to citizens in a timely manner.

[2] Information that was confidential to the municipality or concerned personal information relating to either the municipality's staffs or citizens.

elements of the story in English on a large sheet for plenary presentation. This phase took about half an hour. The plenary presentation of the first four stories took about 90 minutes, as the presentations invoked a lot of discussion.
Because the four stories were quite similar, albeit interesting in their own right, we asked system administrators to contribute different stories in the second round. This proved to be a difficult task, with a lot of discussion (in Greek). This resulted in another two stories, giving a total of six stories, which completed the morning session of four hours.
After lunch the workshop continued with a discussion on the possible uses of these stories for scenario development, including a discussion on the elements of such a scenario. This discussion will not be reported here.
The experience was not evaluated explicitly, but all participants may confirm a cooperative spirit with an open and inspiring discussion. Some tension arose during the second round of story-telling, because of a lack of clear ideas and criteria for new stories that were 'different' from the first round of stories. This was resolved by granting participants their time for brainstorming and collaborative negotiation. The resulting user stories can be found in Annex 5.

#### *4.2.2.1 Workshop Analysis*

The six stories permit to depict two activity systems, as introduced in Section 4.1, that each characterise activities with respect to cybersecurity issues from different points of view: that of the user of services (members of the departments of the municipality, in their role as customers) and that of the IT-department in particular (in their role as actors). We can easily understand that both activity systems interact in the case of cybersecurity issues. Please keep in mind that our interpretations are tentative, based on a limited number of stories. Nevertheless, the views played out in the stories seem coherent enough to warrant interpretation. Our interpretations have been checked with the users.

##### 4.2.2.1.1 The user activity system

The user activity system that we describe is a generalisation, and might be different for each department in the municipality. These differences have not appeared as significant, given the limited number of stories that we have been collecting. Like any activity system, it represents multiple voices (as in points of view, interests or traditions, positions), it has been shaped by the history of the unit and of the municipality, and can contain tensions and contradictions, which can be a motivation for change (Engeström, Expansive Learning at Work: Toward an activity theoretical reconceptualization., 2001). We have to be careful, they should be taken as *possible sources* of tension. Figure 4 depicts this user-activity system.

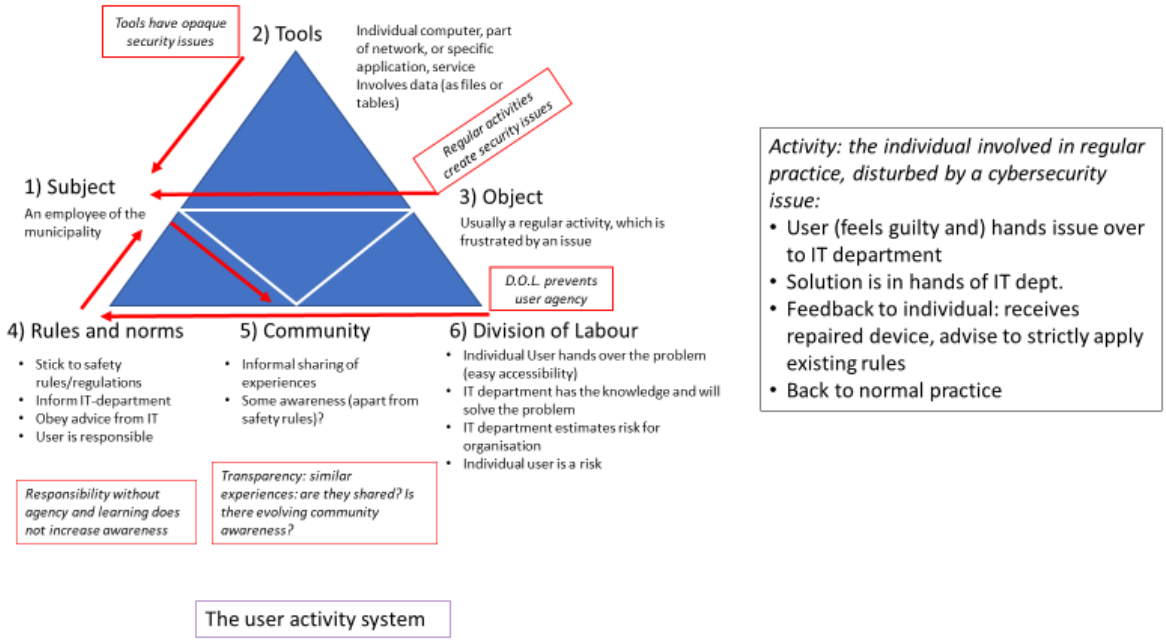



*Figure 4:* The user activity system characterises the activities of users of services who produced stories of cybersecurity issues. Red arrows indicate possible tension.

As can be seen, there is a *subject*, which is the generic user of technological services who has the *objective* of making use of a computer (the tool) as a regular part of the job, but is faced with some obstacle so that the regular activity cannot be performed. This is the initial issue and this gives rise to a shifted objective: the resolution of the technical issue. Characteristically, this user does not have the knowledge (tools) to resolve the issue, the user needs the IT-department for this. Enter activity system 2, depicted in Figure 5, and now we can say there are two systems operating with the same objective: resolution of the issue, but according to different principles, and with different tools.

In the case of this municipality, the subject is part of the *community*: all users within a department, or in our case with a limited number of stories, all customers in the municipality. These users frequently interact, but we do not know the extent to which these interactions concern cybersecurity. In other words, their stories show that our users may have some awareness of risks, but there is no general (formal) procedure for sharing cybersecurity issues with all members of the community, or within a particular department. This means that some issues may reappear, with a different user. We find examples of the tensions related to this lack of transparency in all stories.

What users should all share are the *rules*: there is a clear set of safety-regulations set out by the IT-Department for safe cyber behaviour. The most important one is: "*all users are warned not to open e-mails from unknown senders or without a subject or with attached files in .zip or .exe format*". We suppose this list of regulations covers all situations so far, it probably is updated with every new case, when necessary. A general rule is that all cybersecurity issues should be reported to the IT-Department, who have the knowledge to adequately deal with them. The rule is for the benefit of the community: if I do not report then the community is endangered. But this rule also creates possible tension for the user: if I report then people may think I am a sloppy user (whose behaviour is bad for the community). Finally, there is the awareness issue for the community: what is shared about certain events with the community?

The *division of labour* is very clear: all cyber issues will be handled by the IT-Department. They are seen as competent, reliable, quick, and are especially good at estimating the risk for the organisation and taking the necessary measures. On the other hand, our user knows to be seen as a risk, a possible source of mistakes, the user needs to stick to the regulations to avoid making these

mistakes. The procedure is clear: the user with the issue hands over all responsibility, and then will be returned a repaired machine as soon as possible. If needed, other machines within the system will be handled as well.
This leads to the final part of the activity system, which is the *tool*. The user, any user, probably understands how to operate the machine as an instrument for doing some jobs. As a tool, it functions in so far it is needed. Part of the meaning of the tool is doing the job correctly. If this fails, then the machine is not a tool anymore, but an obstacle. What is missing for the user, as part of the tool, is the knowledge about the system. We already said, above, the rules and the division of labour do not assume that users possess any agency for remediation. In the current system, they are not supposed to know much. It is an open question what awareness might support better handling of issues from the user side, or less tensions when handing over the tool, and if this is desirable.

#### 4.2.2.1.2 The IT-Department activity system

This system is depicted below in Figure 5. Here, the *subject* is a member of the IT-Department (5 people) that handles all issues with cybersecurity. The department has one head, respected for his precision and expertise, the other members are equal. They are member of (at least) two *communities*: the first is the municipality that they work for, and maybe some smaller municipalities in the area. This community is the main client of the IT-Department, and the well-being of this community is the main reason for their services. There is frequent exchange of issues, ideas and solutions, but (as we assume) not in a systematic manner. The second community is that of IT-specialists with a similar task description, including cybersecurity response teams, task forces and authorities. This second community is important for development of expertise and for consulting possible solutions for issues, but also for conveying information about (new) threats to cybersecurity. Sharing activities with the community of professionals was not explicitly addressed in the story workshop, albeit there was clear mention of consultation of blogs and forums where active communication within this community mostly takes place. It is unknown how frequent the members of this department exchange feedback with other members of the community of their profession (the second type).
The objective that is shared with the user activity system is the resolution of cybersecurity issues. Perhaps in a more general sense such objectives give rise to development of tools: experiential knowledge for knowing how to act, including where to find knowledge, expertise about networks and systems, safety rules and antivirus solutions such as patches and cleaning software. Tools are mainly the domain of expertise for this activity system.

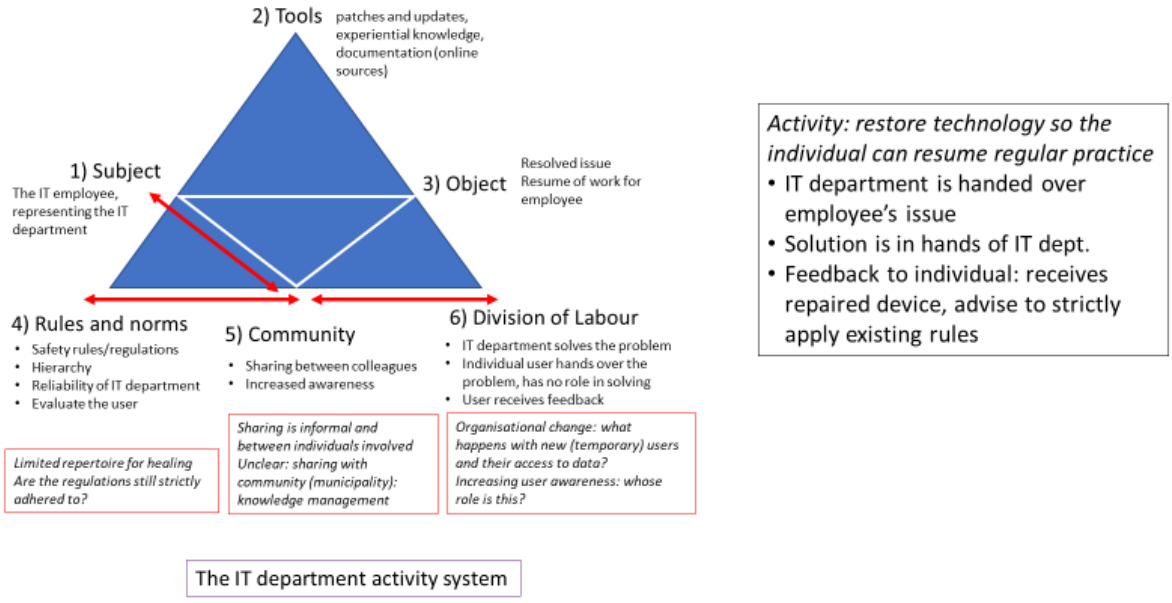



*Figure 5: The IT-Department activity system*

The rules and norms the IT-Department maintains are monitoring safety behaviour, and providing high quality services to the users. It seems they are doing fine, but it was difficult to discuss uncertainties in this respect.
Concerning the *division of labour* (already discussed in Section 4.2.2.1.1) they raised an additional point in story 6: due to increasing flexibility on the job market and availability of jobs, it may be possible that more and more people will be employed on a temporary basis. These people may have different *norms*, with respect to safety regulations, but also with respect to the importance of the community.

#### 4.2.2.1.3 Summary of tensions in the activity systems

At first sight, one might localise the main source of tension in technology: a system, or computer that has an issue. In our analysis, the tension also is sought in the underlying components of the organisational activity system. This means that the main source of tension is not just a *malfunction* of the technology, it is the fact that (1.1) *users experience opaqueness of security issues*: generally, users do not understand the nature of the problem, and therefore rely on the expertise of others for resolution, but also for awareness about causes and the severity of the threat. This applies to most users of technology, we do not assume this is specific only for our current group of participants.
More specific for our users is that tension can be caused because their (1.2) *regular user activities may create security issues*, meaning for example that it can be in the job description of some employees that they have to open all emails, or that they have to sometimes work with files from external sources. These first two sources of tension may contribute to the idea that some people have dangerous jobs. It is an open question how to handle these potential sources of tension, if they can be handled at all.
Three further potential sources of tension relate to how cybersecurity issues are dealt with in the organisation. The main potential source of tension of a service-user is that while these users are assumed responsible for mistakes, the division of labour is such that (1.3) *users experience no agency in dealing with cybersecurity issues*, so their learning is limited. They are merely reminded about adhering to the rules, as a consequence (1.4) *user awareness is not addressed*. Moreover, there is a transparency issue (1.5) *the community (of other users in the municipality) remains*

*uninformed* about all issues and their potential dangers. The main source of information is informal communication, which suggests a close community, but also a possibly somewhat unaware (and therefore insecure) community of users. Note again, this interpretation is based on a limited set of stories of incidents, and we did, for instance, not ask for stories in which users were successful in resolving the issue on their own, and sharing the outcome and all necessary characteristics with all others in the municipality, including their IT-Department.

We discuss here possible tensions in particular, as a source for further growth and possibilities for change. We need to stress that there are many strong points and assets as well. The stories reveal that the IT-Department is very easy to reach, always ready to help, are competent as individuals, and also as a team, and seem very efficient at doing their job. Their organisation seems very adequate and internal lines are short, with frequent (informal) communication between its participants.

The second activity system also reveals sources of tension, that do not relate to the user as an individual (who is now represented as the community of users), but more to organisational matters. Potential tensions between components in this activity system are reciprocal: both components seem to suffer. The sources of tension concern sharing, healing, and trust. The first potential source of tension concerns individual users: the causes of a cybersecurity issue are evaluated, with user behaviour as a possible component, but (in addition to personal warmth and empathy, and reminders about sticking to the rules) there seem to be (2.1) *no healing procedures implemented*. This means that there is no safe bet that the user will have learned much from the issue, so the user will remain a source of tension of the IT-department. In a larger sense, the same applies to the user community, in the sense that most sharing seems informal, and on an individual level (between the user with the problem and the administrator who handles the problem), there are (2.2) *no sharing procedures implemented with other members of the municipality*. This means that the municipality is insecure about potential issues, and the IT-department is insecure about the behaviour of the other departments. The third type of tension involves trust, especially concerning knowledge management. The IT-department experiences (2.3) *insecurity about new users having access to sensitive information*, but there is the reverse tension by users relying so much on the expertise of the IT-department that they cannot live without them. As a consequence, new and longer standing users alike, they are likely to make mistakes, and longer standing users, who are in daily contact with the new users, cannot evaluate the dangers of these new users having access to sensitive data.

## 4.3 Second Soft Systems Workshop in the Municipality of Rome (19.11 - 23.11.2018)

The third workshop in Roma Capitale (RC) commenced on November 19th 2018. The workshop participants were the following:

| **Organization** | **Participant** |
|---|---|
| University of Oulu | Christian Wieser |
| University of Vienna | Thomas Schaberreiter<br>Veronika Kupfersberger |
| CARIS Research Ltd | Christopher Wills |
| Wise&Munro | Jerry Andriessen |
| CloudPartners | Kim Gammelgaard |
| 3rdPlace | Matteo Bregonzio |
| Cesviter | John Forrester |
| Municipality of Larissa | Thanasis Poultsidis |
| Municipality of Roma Capitale | Arianna Bertollini<br>Simona Stoklin<br>Andrea Quatrini |

| | |
|---|---|
| | Luca Iezzi<br>Roberto Massimiliani<br>Massimiliano Zanchiello<br>Ivano Ottaviani<br>Ivan Bernabucci<br>Mauro Melella<br>Walter Duca<br>Raffaella Pullano<br>Mirella Rondinelli<br>Claudio Baffioni<br>Stefano Vallocchia<br>Andrea Boggio (Fastweb)<br>Antonio La Malfa (Accenture) |

In addition, for the story telling workshop part several end users of RC services (all employees of RC) were present, but since they are not part of the core CS-AWARE team, their names are not made public in this document for data protection reasons.
Section 4.3.1 will detail the system and dependency analysis focused workshop part, and Section 4.3.2 will detail the end user focused story telling workshop including the respective main results of each workshop part.

### 4.3.1 Part 1: System and dependency analysis

Similar to the workshop in Larissa, the analyst team had identified the most relevant rich pictures (found in Annex 2 of CS-AWARE Deliverable 2.1), which were most relevant to define the initial understanding of systems and dependencies modelled in the GraphingWiki based graph found in the non-public Annex 9 of this document. The most relevant rich pictures were:

- Team 1 RP 1
- Version Team 1 RP 2A-V2
- RP IAM
- Version Team 4 RP 2
- Version Team 4 RP 3
- Version Team 4 RP 3-V2
- RP DMZ detail

The goal for this workshop round was to deepen the understanding of the relevant business processes for the services that CS-AWARE is looking at, refine our understanding of the systems and dependencies based on the initial GraphingWiki graph, and finally map the processes to the systems and dependency graph in order to identify the relevant information flows.
The workshop began with an introduction by Raffaella Pullano. Thomas Schaberreiter followed with an overview of the CS-AWARE project for the benefit of representatives from the Agenzia per l'Italia Digitale (AGID)[3] who were present. Chris Wills then gave an overview of the conceptual model and root definition stages of SSM, similar to the slide set used in Larissa found in Annex 2 of this document. A decision was taken to look more closely at the sub-processes relating to the SUET system and the associated Identity Access Management system (IAM).
The RC team offered to repeat the presentation on SUET that had been given in the preceding workshop. A copy similar to that presentation can be found in Annex 4 of Deliverable 2.1. The

[3] https://www.agid.gov.it/

SUET processes the compilation and submission of building applications. These can be made either by citizens or by professionals (architects or civil engineers). The relevant slide of the presentation that helped to identify the main SUET processes can be seen in Figure 6, which helped the team to establish a baseline for the CATWOE analysis. The first two sub-processes set out in the slide, those of "Drafting and submission" and "Work processes of an instance". Drafting a submission (submitting an application by citizens and/or their approved technicians) in SUET results in the creation of an "instance" i.e., a live application, which is then checked on several levels by RC employees, and roughly translate to following actions:

- Administrative verification (is the application lawful?)
- Technical examination (does it meet building and technical regulations?)
- Pay management (has the applicant paid the correct fee for the application?)
- Final result (has the application been granted or denied permission?)
- Output act (recording and disseminating the outcome of the application)

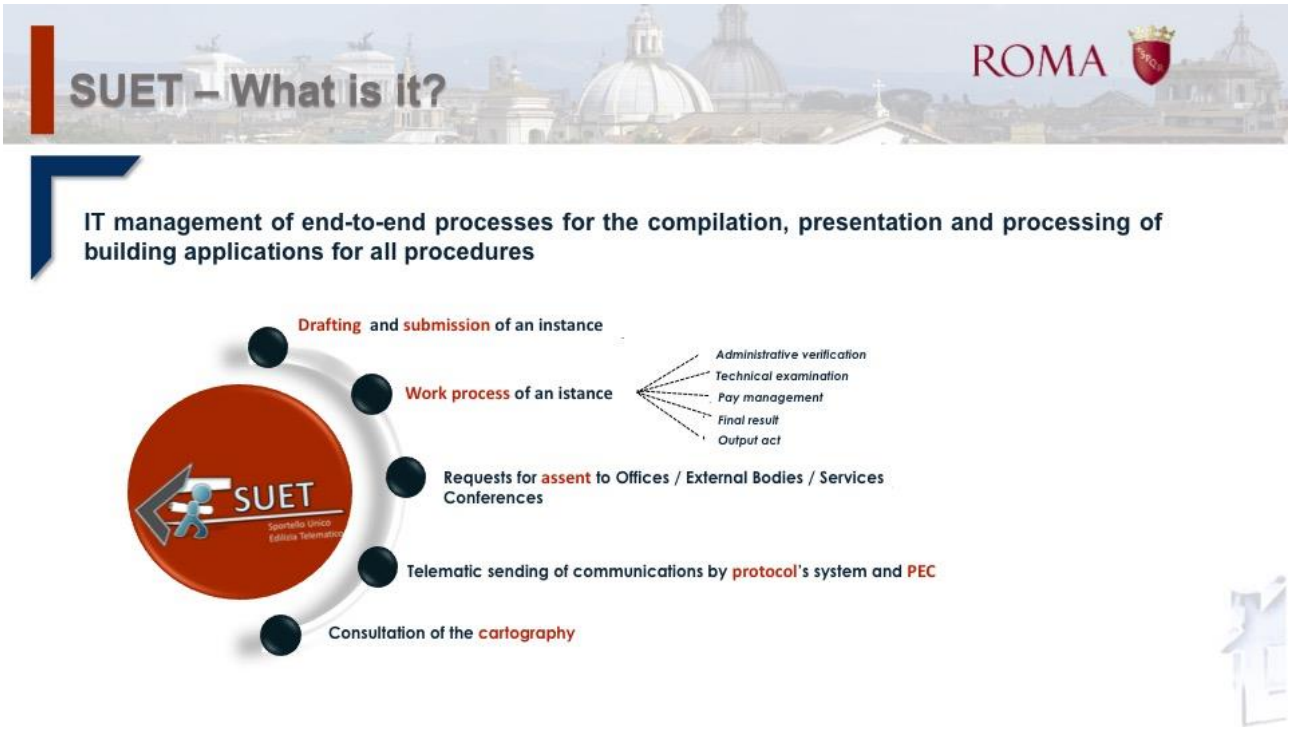



*Figure 6 SUET processes*

In order to sort the ideas and identify the most relevant processes, following high-level usage overview of SUET (including the involved IAM procedures access management) was established, based in part on a live demonstration of SUET and related IAM interactions: Citizens and professional applicants gain access to SUET via the Internet. The Identity Management System (IAM) authorises their access. The Identity Manager manages the lifecycle of users. The Access Manager manages access rights. Applicants potentially have several roles within SUET; they can be citizens, professionals, employees and employee's managers. Role management data is stored in the same database as application data. The LDAP databases for access and identity manager are synchronised. The Access Manager (AM) DB is read only, the Identity Manager (IM) is both read and write. Data entered into the AM is checked with the IM.
Applicants can upload documents and PDF's to the SUET system. SUET is therefore potentially vulnerable to cyber attack. RC employees have access to SUET, however this access is via the Intranet where all users have already had their identities and access credentials certified as correct.

The payment system is separate from SUET. A citizen or professional applicant pays for an application via the payment system. The payment system generates a payment code that the applicant then enters into SUET. The SUET system checks to confirm that the code is correct and if so, the system authorises the application being made by the applicant. There is a separate national system that is used by contractors and suppliers.
Based on this initial understanding, following relevant processes were identified for the SUET service:

1) Drafting and Submission
2) Verification and Approval
3) Employees/Managers Enablement

For the IAM service, following processes have been identified:

1) Registration
2) Authentication
3) Authorisation
4) User management

The CATWOE analysis for all those identified processes can be found in Annex 6 and Annex 7 of this document, respectively.

Following the CATWOE analysis, it was decided to review the system and dependency graph to identify any wrong interpretations of the rich pictures from the previous workshop and, where necessary, refine our understanding. Thomas Schaberreiter guided the workshop participants on a walk-through of the GraphingWiki graph, and the relevant original rich pictures from last year have been pinned to the wall for reference. Together with the RC team many changes and additions were made to the GraphingWiki graph, based on discussions facilitated by the analyst teams and the expertise of the workshop participants. Based on the analyst's experiences of this exercise, the GrapingWiki based representation has proven to be an excellent tool to compress a great amount of information into a simple and intuitively understandable graphical representation. Both the original graph and the revised graph can be found in the non-public Annex 9 of the document.

Once the workshop participants and the analyst team were satisfied to have reached a satisfactory level of understanding regarding the systems and dependencies, the last part of the dependency analysis focused workshop was concerned with mapping the identified business processes to the system and dependency graph, identifying the relevant information flows and transformations associated to each of those processes. Furthermore, it was reviewed for each relevant information flow if the previously identified monitoring points would be sufficient to capture the relevant flows and transformations in the CS-AWARE cybersecurity context. While it was concluded that all the potential information sources that have been identified already in CS-AWARE Deliverable 2.1 are still valid and most likely are able to capture the required information, some additional information was given by the RC team as to how to best collect this information (e.g. several log sources have been modified since the last workshop in such a way that they can be collected from a centralized log repository). The resulting information flow graphs for each relevant process can be found in the non-public Annex 9.

#### *4.3.1.1 Workshop Discussion and Results*

The outcome of the third workshop in Rome was that the analysts gained a clear understanding of Rome's networks, systems and processes. This understanding was underwritten and confirmed by

the Rome's personnel who participated in the workshops. The analysts were able to identify the key systems and processes in Rome (those that either stored, processed data that was mission-critical to Rome[4] or stored or processed sensitive or personal information[5]), as well as the key processes and information flows related to those systems. The analysts were able to identify the most appropriate locations in Rome's networks and systems where data could be monitored without compromising the privacy of citizens in breach of the GDPR. It should be noted that the analysts found the GraphingWiki based system and dependency representation an extremely helpful tool to gain a better understanding of the system setups and relevant information flows through those systems. The greater complexity of the systems as compared to Larissa made this type of representation even more relevant in this case, since an overview understanding (or anchor point) could always be easily maintained while discussing technical aspects in different parts of the systems. Especially in the edge cases, where responsibilities for different parts of the systems shift from one department/contractor to another, the specific connections between those parts could be identified and discussed more easily.

### 4.3.2 Part 2: End user focused sessions

The municipality for workshop II is a very large capital. Present at workshop II were a number (between 10 and 15) of system administrators who had also participated during the three previous days in the SDA workshop. The role of these participants within the municipality was generally not that of Internet Services, they could also be managers of contracts, or representatives of private parties that were responsible for a particular component of the system. The local team leader had engaged 3 additional public administrators, from the department of the organisation that handled European contracts. Four researchers from the CS-Aware project also took part, as moderators, and we gratefully acknowledge the contributions from the local team leader of workshop I. Initially, all participants were divided in four groups of 3-5 members each. As the meeting evolved, some people left, then came back or not, and the original groups mingled into different compositions, according to the procedure introduced in Section 4.1.

About four months before the workshop we asked (through our Ancitel contact) for potential participants by email to send us short stories of cybersecurity experiences. With this preparatory assignment, we hoped to focus the awareness process on an individual level in order to give participants space for their own ideas. We did not receive any stories, so it was assumed that the participants came relatively unprepared. It should be noted that RC conducted a questionnaire among a larger subset of RC employees, the results of which are interesting in itself, but insignificantly relevant in preparation for the story telling workshops.

The workshop session started with an explanatory talk by Jerry Andriessen, all participants from the municipality were asked to individually generate an experience that involved some issue with the cybersecurity of their organisation. It was free for them to write it down or not. After ten minutes participants were asked to join their group. The task of the group was to develop the story by adding topics to the experience and to provide these topics with more depth. The groups could discuss in their native language, but they were asked to put the elements of the story in English on a large sheet for plenary presentation. This phase took about 45 minutes. The plenary presentation of the first three stories took about 30 minutes.

The group appeared to be full of stories, so, after a coffee break, we asked them to generate more stories in a second round. This resulted in another three stories, giving a total of six stories, which

[4] Mission-critical in that it would either undermine the finances of the municipality or negatively impact the ability of the municipality to deliver key services to citizens in a timely manner.

[5] Information that was confidential to the municipality or concerned personal information relating to either the municipality's staffs or citizens.

completed the morning session of about three hours. The experience was not evaluated explicitly, but all participants may confirm a cooperative spirit with an open and inspiring discussion. From the view of project management, this positive experience could be a fertile ground for a workshop during a next meeting. The resulting user stories can be found in Annex 8.

#### *4.3.2.1 Workshop Analysis*

We consider those users with issues as an activity system. This is further explained in Section 4.1. It should be noted that for the interpretation of the stories in workshop II, there is a lack of stories from actual users. Therefore, our interpretation of the user activity system is incomplete and tentative. This means there may be more issues and possible stories.

##### 4.3.2.1.1 The user activity system

The user activity system that we describe is a generalisation, and might be different for each department in the municipality. These differences have not appeared, given the limited number of stories that we have been collecting. Like any activity system, it represents multiple voices (as in points of view, interests or traditions, positions), it has been shaped by the history of the unit and of the municipality, and can contain tensions and contradictions, which can be a motivation for change (Engeström, Expansive Learning at Work: Toward an activity theoretical reconceptualization., 2001). We have to be careful, such tensions should be taken as *possible sources* of tension. Figure 7 depicts this user-activity system.

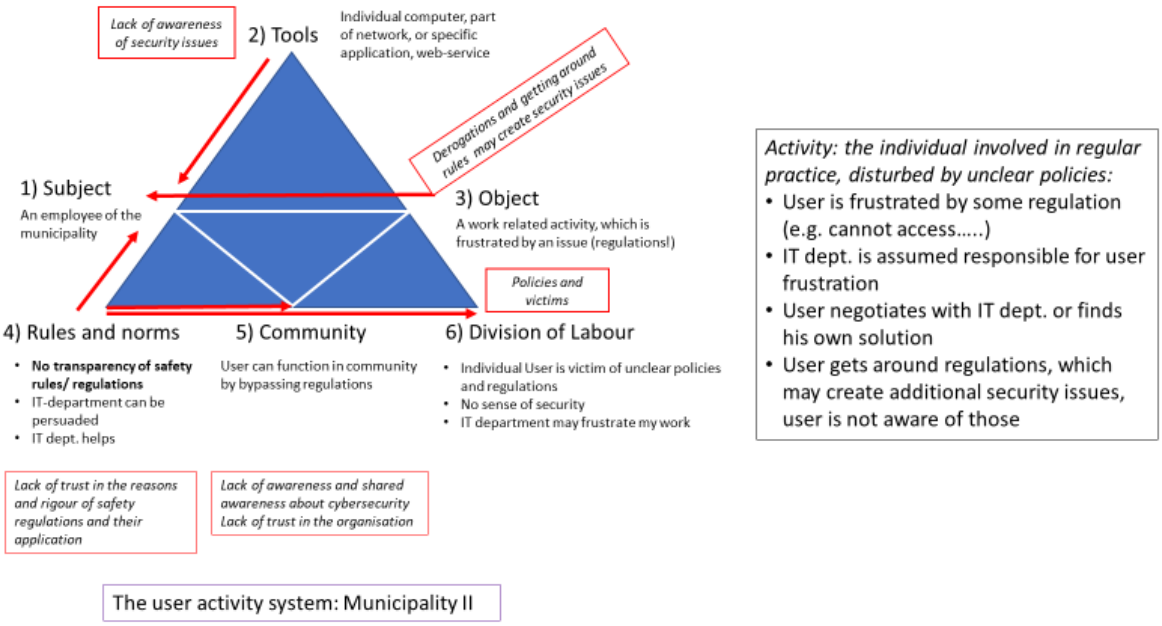



*Figure 7:* The user activity system, characterises the activities of users of services who produced stories of cybersecurity issues. Red arrows indicate possible tension.

As can be seen, there is a *subject*, which is the generic user of technological services who has the *objective* of making use of a computer (the tool) as a regular part of the job, but is faced with some obstacle so that the regular activity cannot be performed. This is the initial issue and this gives rise to a shifted objective: the resolution of the technical issue. Characteristically, this user does not have the knowledge (tools) to resolve the issue, the user needs the IT-department for this. If we compare the current municipality with the previous one, we see that the issue is different. In the current municipality, the users seem most frustrated by encountering obstacles in their professional activity, because there are regulations preventing their access to websites or the use of an

application they need for their job. Characteristically, users try to get around this issue, either by negotiating with the IT-department, or by using their own technology. The first solution does not resolve the general issue for the municipality, but only for selected users. The second solution may give rise to additional cybersecurity issues.
We know that users also encounter the more regular cybersecurity issues, such as phishing or viruses. An informal questionnaire issued by the the RC team, with about 44 respondents shows the distribution of such issues. These were not raised during the workshop, we do not know to what extent users regard these as very problematic. We also do not have much information about the professional communities in which they are functioning.
The core of frustrations by the users reveals some imperfections of the rules and norms. Awareness of safety rules is beneficial for users, and as is the case in many contexts, they acquire such awareness by trial and error, and through interactions with others. In the current case, regulations are experienced as lacking any logic, or this logic is not understood. There is a clear tension between the professional needs of regular users, and the rules and regulations that are supposed to support their sense of security. This relates to the norm that rules are to be bypassed. This lack of trust in safety regulations may also relate to lack of trust in the policies of the organisation. It can be assumed that this is typical for many bureaucratic organisations, such as universities, in other countries as well.
The *division of labour* amounts to users sorting out their technical issues, if possible, with the support of the IT-Department. The IT-department are seen as part of the organisation, hence there maybe is not much doubt about their competencies, but there is doubt in their procedures and the application of policies. Security issues seem less important for users than the frustration of not being able to do your job. As a consequence, we do not think their level of awareness of security issues is very high.
The user, any user, probably understands how to operate the machine as an instrument for doing some jobs. As a tool, it functions in so far it is needed. Part of the meaning of the tool is doing the job correctly. If this fails, then the machine is not a tool anymore, but an obstacle. What is missing for the user, as part of the tool, is the knowledge about the system regulations. It is an open question what awareness might support better handling of issues from the user side, or less tensions when meeting a technical issue, and if this is desirable.

#### 4.3.2.1.2 The IT-Department activity system

This system is depicted in Figure 8. Here, the *subject* is a member of the IT-Department (size unknown) that handles all issues with cybersecurity. The department in a larger sense is a very complex structure within a very large municipality. Many services have been outsourced, and as a consequence, no one has full overview or full responsibility over the network. It is unclear how communication between the various stakeholders takes place, or what communities in a smaller or larger sense they are involved in.
The objective that is shared with the user activity system is the resolution of cybersecurity issues. Perhaps in a more general sense such objectives give rise to development of tools: experiential knowledge for knowing how to act, including where to find knowledge, expertise about networks and systems, safety rules and antivirus solutions such as patches and cleaning software. Tools are main the domain of expertise for this activity system. The lack of insufficient funds for security relevant upgrades usually seems to be a concern in this activity system. Dangers for users are always lurking when they have to work with outdated versions of system software.

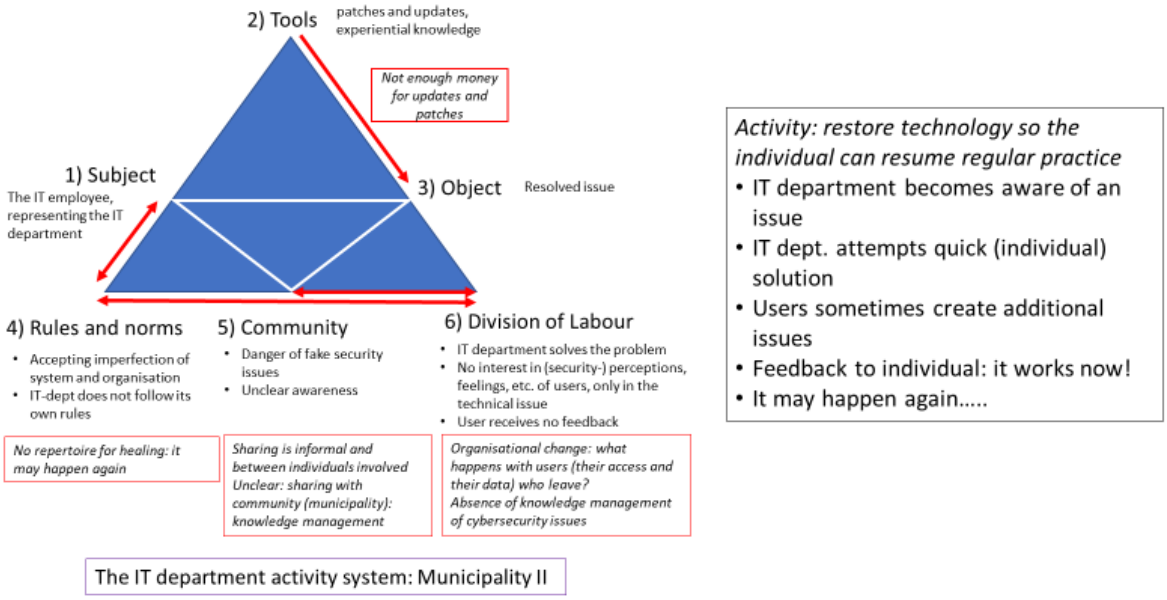



*Figure 8: The IT-Department activity system for workshop II*

The rules (and norms) the IT-Department maintains are about monitoring safety behaviour, and providing services to the users. Obviously, the complexity of the organisation requires that many services are outsourced to smaller departments or organisations. Here, there seems to be a general norm that the system as a whole is too complex, and we should accept imperfection to the extent that not all policy regulations are in the interest of cybersecurity. There may also be some lack of trust in the good intentions of the organisation management, but it looks like the IT-department is still able to provide quick services to users with problems. These services are provided on an individual basis, there is no follow-up, and there may be no spread of information to other users in case of a security issue. However, there may be employees within the department who engage in some form of information sharing with other employees.

Concerning the *division of labour* (already discussed in the section about users) they raised an additional point in story 4: who is responsible for the administration (access or removal) of users? Isn't it a problem when users leave the organisation but may still have internal access to the system after several months? This again relates to the issue of knowledge management, to users, who seem to have less concern and a lack of awareness for cybersecurity issues, and to their own department, in which the culture favours general regulations (too many) but individual solutions (not shared).

#### 4.3.2.1.3 Summary of tensions in the activity systems

The main source of tension as appeared from the stories was not in the technology itself: the main source of tensions with technology was found in the rules and norms of the organisation. In our analysis, the tension in the underlying components of the organisational activity system. This means that the main source of tension is not just a *malfunction* of the technology, it is the fact that (3.1) *users experience a lack of awareness of security issues*: generally, users do not understand the nature of the problem, and therefore rely on the expertise of others for resolution, but they localise the main source of the issues in the organisation itself: rules and regulations that they do not share nor understand. As a consequence, users look for ways to circumvent the issues that they encounter, which brings additional cybersecurity risks. This means that a main source of tension is that (3.2) *User activities may create security issues*. It is an open question how to handle these potential sources of tension, if they can be handled at all.

Three further potential sources of tension relate to how cybersecurity issues are dealt with in the organisation. The rules and regulations are such that (3.3) *users experience a lack of transparency in dealing with cybersecurity issues,* so their learning is limited. Moreover, there is a related transparency issue in that (3.4) *the community (of other users in the municipality) remains uninformed* about all issues and their potential dangers. Our stories tell us that users see themselves as (3.5) *victims of failing policies*. Note again, this interpretation is based on a limited set of stories of incidents, and we assume that some users can be successful in resolving the issue on their own, and then sharing the outcome and all necessary characteristics with all others in the municipality, even including their IT-Department.

The second activity system also reveals sources of tension, that do not relate to the user as an individual (who is now represented as the community of users), but more to organisational matters. Potential tensions between components in this activity system are reciprocal: both components seem to suffer. The sources of tension concern (4.1) *lack of resources*, (4.2) *lack of concern for users*, and (4.3) *lack of knowledge management*. Firstly, a lack of concern for updates is explained by a lack of resources. This leads to concerns for cybersecurity which are not about technology, but about the organisation. This implies that cybersecurity concerns are not as imperative as they should be. Please note that this may differ for various outsourced components.

The conclusion that cybersecurity is not the first concern of the IT-department is reinforced by the following observations: a) there is lack of concern for the wellbeing of the users: were they helped, what happened with their issue, what happened with the data they lost?; b) there is no follow-up after an issue has been resolved, not to all users, nor (it seems) to others within the department; an issue can easily happen again; c) repair and support is on an individual basis, it is unclear if there are policies, and mistakes can be made without clear personal consequences; d) there are no clear procedures in place for users that have left the organisation; there seems to be (4.4) *no management of users that do not work for the municipality and have access to sensitive information*.

## 4.4 Conclusions drawn from the story telling workshops in Larissa and Rome

We identified some sources of tensions in the user- and system administrator- activity systems, in the stories collected during the first story workshops in the two municipalities. Although it may seem there are some similarities between the municipalities in this respect, in fact we are talking about very different systems for dealing with cybersecurity. In this section, we suggest some recommendations pertaining to the CS-AWARE cybersecurity solution, especially concerning the scenarios for its implementation.

When we use the term “users” it should be clear we refer to customers of services, that is the professionals who work for the municipalities in any of the departments. When we speak about IT-administrators, or system administrators, or actors, we refer to the professionals who work in the IT-department of the municipalities. Some IT-administrators are directly involved in resolving cybersecurity technical issues, others have administrative roles.

The main conclusion that is confirmed again from this small collection of stories is that any technological solution requires considering its users. Although the CS-AWARE solution specifically targets the system administrators, and their awareness in a general sense, we think that in order to have any impact, this awareness needs to consider the users of the services, the policies for safety regulations, and the potential dangers that are part of any internal organisation. We have seen examples of what can happen when policies are not coherent. Also, we highly recommend for system administrators to include the users in any feedback loop, to help them understand the reasons for their issues with cybersecurity, and to make them realise the consequences of some types of behaviour, even if it was someone else who experienced an issue.

This being said, we provide following suggestions for the areas of the project:

- The System and Dependency Analysis (SDA): The second round of SDA workshops applied a soft systems methodology to identify the processes run on two critical servers employed at each municipality. These processes will be linked to concrete work processes inherent to the activity at some department of the municipality. We have now more insights into the issues that customers and actors are facing. We suggest that for these selected activities a workshop will be organised for getting more specific insight in the needs and barriers of users involved in this particular activity. This can be combined or integrated in the third SDA workshop. In this way the use of data sources most relevant to user activity can be understood more precisely in terms of user context.
- The construction of pilot scenarios (D2.2): The SDA outcomes will be used to define a first series of pilot scenarios. These scenarios define step-by-step the information flows through parts of the system that will be monitored. In this case we would underline the importance of system administrators interactively questioning the system, instead of waiting for reports to come. In addition, evolving trust seems to be highly correlated with the degree of certainty of a monitoring component reliably reporting “no issues”. Interactive consultation has implications for the user interface as well. In the pilot phase, the roles of actors in managing the information flows will be considered in appropriate use cases, which are outlined in Section 5 of this document.
- The deployment phase (D5.1): Deployment scenarios address the needs and barriers of users, which are expected to evolve over time when our solution is implemented. This means that these scenarios need components that involve precise expectations with regard to such needs and barriers, such as clear objectives, success criteria, and desired behaviour of administrators and users with respect to the objectives.
- The evaluation of the CS-AWARE solution and its use (D5.2): Evaluation of the deployment scenarios requires formulation and testing of success criteria involving users, especially concerning cybersecurity awareness, information sharing and self-healing. This evaluation should address in some way the knowledge management and transparency issues in the municipalities that were revealed by the story workshop. This involves:
    a. User management: adding or removing users, access rights of old and new users , in relation to insider attacks
    b. Feedback and reporting on incidents, to other users or within a department, in relation to awareness of actors and customers
    c. Prevention policies and monitoring of prevention effectiveness, for awareness and healing
    d. Timely updates of main system components

- The story report (D5.3): The story workshop can be seen as a first step towards further collection of richer stories that will also describe changes in user experiences as a result of the interventions. We feel confident that we will be able to collect useful stories from relevant participants in next workshop sessions.

## 4.5 Pilot Scenario Definition

Based on the results of the SSM workshops and storytelling workshops in the Municipalities of Larissa and Rome, the pilot scenarios for CS-AWARE will be defined in this Section. It should be noted that while a general description of the approach taken towards scenario definition will be

presented, the concrete scenarios can be found in the non-public Annex 9 due to the sensitive nature of this information and the potential security implications of publishing it.

Based on

- the results of the initial risk analysis that concluded that the data managed by LPAs is the most valuable asset
- the system and dependency analysis results that has shown that following the information flows through the systems can give valuable insight into the systems operations
- the process analysis that has shown us the importance of data flows and transformations for the day-to-day operations in Municipalities
- the story telling workshops that have given us insights into the day-to-day problems and interactions of end users (end user activity system) and administrators (IT department activity system) with the systems in terms of cybersecurity, according to their critical interactions with the relevant processes that have been identified

it was concluded that the piloting scenarios should be modelled according to the information flows that the processes of the identified critical services produce. Knowing and understanding the information flows that run through the systems, enables the identification of relevant monitoring points for each of those processes. Furthermore, having identified the data transformations of each process enables the narrowing or focussing of the data that needs to be collected from each information source in order to determine and analyse it for cybersecurity relevant deviations from normal operation.

A graphical representation of each of the possible pilot scenarios and, where applicable a detailed analysis of the scenario, can be found in the non-public Annex 9. Having identified the piloting scenarios, it is possible to define meaningful use cases on top of the scenarios that will allow to raise awareness according to those use cases. The use case definition can be found in Section 5.

# 5 Definition of CS-AWARE cybersecurity awareness use-cases

In order to narrow the context of what kind of cybersecurity awareness CS-AWARE will create during the project, it was decided to define relevant use cases that can be applied on top of the pilot scenarios defined in Section 4.5. Each use case has the characteristic that it differs in the type of cybersecurity relevant aspect that is analysed and/or the type of data sources and data fusions required to draw conclusions in terms of cybersecurity awareness. An influencing factor in defining the use cases were the results of the story telling workshops, since those gave us insight into the actual problems that end users and administrators are concerned of on a day-to-day basis. Many of those concerns are reflected in the chosen use cases and we expect that the on-line monitoring and awareness aspect of CS-AWARE will assist administrators in addressing such problems faster than is possible currently. The use cases are listed in Table 5.

*Table 5: The CS-AWARE use cases*

| |
|---|
| **Vulnerability use case**: The vulnerability use case relies on information from publicly available vulnerability databases, as well as information about software and/or hardware appliances of LPA systems that are relevant to the identified pilot scenarios. The analysis engine will map known vulnerabilities to installed appliances and assess the severity based on information available from the relevant data sources. The vulnerability use case is unidirectional in the sense that only known vulnerabilities will be mapped to installed appliances. CS-AWARE will not actively scan for |

| |
|---|
| unknown vulnerabilities in the LPA systems (e.g. using vulnerability testing techniques like fuzz testing) that would be shared with the relevant communities via the information sharing component – CS-AWARE will rely on already known and classified vulnerabilities and map those to concrete LPA appliances. |
| **Suspicious behaviour monitoring:** CS-AWARE will scan for suspicious patterns from LPA log sources (database logs, application logs, security appliance logs, network logs) relevant for the identified pilot scenarios, try to map and classify this behaviour according to information gathered from relevant threat intelligence platforms and assign a severity based on this information. The quality of the log sources is of special importance for this use case, in order to achieve high quality analysis results. If possible, self-healing will be performed based on information retrieved from relevant external sources (or CS-AWARE internal policy database), otherwise awareness will be raised through visualization for decision support. If a suspicious pattern that was detected in the LPA systems cannot be classified to any known threat shared by threat intelligence communities, the possibility for sharing this information with the relevant communities will be available – after asking consent from LPA operators/administrators via the CS-AWARE interface. |
| **General security warnings:** If relevant external information sources (e.g. CERTs or social media sources) distribute general security warnings about cybersecurity relevant incidents (e.g. currently ongoing large-scale attacks), the analysis engine will assess and rank its applicability to the LPA context based on the information about the pilot scenarios, assign a severity to it and visualize it via the CS-AWARE interface to act as decision support for LPA operators/administrators. |
| **Analysis of potentially malicious IP or DNS entries:** At the time of writing of this document, the CS-AWARE project policy is to anonymize all personal data at source. Since IP addresses and DNS entries are classified as personal data under GDPR rules, there are ongoing discussions to change this policy to allow collecting and analysing IP and DNS entries from LPA sources (including the definitions of proper GDPR policies that allow handling of this data). If it is decided to use IP and DNS, one use case of CS-AWARE will be to map suspicious behaviour to IP or DNS entries in LPA systems to relevant information sources that provide blacklists for known malicious entries. Similarly blacklists can be checked against IPs or DNS owned by the LPAs to see if malicious activities originate from LPAs. This information can be used for raising awareness through visualization, or for self-healing to (semi)automatically block malicious entries. Furthermore, sightings of activity originating from blacklisted IPs as well as malicious behaviour originating from IP/DNS entries that are not listed in any relevant blacklist, can be shared with the relevant communities. |

# 6 Bibliography

Baker, M., Andriessen, J., Lund, K., Amelsvoort, M., & Quignard, M. (n.d.). Rainbow: A framework for analysing computer-mediated pedagogical debates. *International Journal of Computer-Supported Collaborative Learning, 2*(2-3), 315-357.

Engeström, Y. (1987). Learning by Expanding: an activity-theoretical approach to developmental research. *Helsinki: Orienta-Konsultit*.

Engeström, Y. (2001). Expansive Learning at Work: Toward an activity theoretical reconceptualization. *Journal of Education at Work, 14*(1), 113-156.

Engeström, Y., Miettinen, R., & Punamäki, R. L. (1999). Perspectives on Activity Theory. *Cambridge University Press*.

ENISA. (2017). ENISA Threat Landscape Report 2017. Retrieved 12 2018, from https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2017

Europol. (2018). Internet Organized Crime Threat Assessment (IOCTA) 2018. Online. Retrieved 12 2018, from https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2017

Foot, K. (2001). Cultural-Historical Activity Theory as Practical Theory: Illuminating the Development of a Conflict Monitoring Network. *Communication Theory, 11*(1), 56-83.

Hanson, J. M. (2015). The Admirality Code: A Cognitive Tool for Self-Directed Learning. *International Journal of Learning, Teaching and Education Research*, (pp. 97-115).

Kurtz, C. (2012). *Working with stories* (3 ed.).

Leont'ev, A. N. (1974). The problem of activity in psychology. *Soviet psychology, 13*(2), 4-33.

Meier, R., Scherrer, C., Gugelmann, D., Lenders, V., & Vanbever, L. (2018). FeedRank: A tamper-resistant method for the ranking of cyber threat intelligence feeds. *10th International Conference on Cyber Conflict (CyCon)*, (pp. 321-344).

Nardi, B. A. (1996). Activity theory and human computer interaction. *Context and Consciousness: Activity Theory and Human-Computer Interaction*, 1-8.

Snowden, D. (2005). From atomism to networks in social systems. *The Learning Organization, 12*(6), 552-562.

Stahl, G. (2013). Theories of Collaborative Cognition: Foundations of CSCL and CSCW Together. *Computer-Supported Collaborative Learning at the Workplace*, 43-63.

# Annex 1

## Qualitative Analysis of external information sources

### NIS competent authorities

| Quality Indicator \ Source | Enisa | CERT-EU | National Certs (CERT-FI example) | Framework Nationale per la Cyber Security (Italy) | CERT nationale Italia | Aristotele University of Thessaloniki (AUTH) CERT (Greece)/ Greek School Network CERT | Europol/EC3 | Interpol |
|---|---|---|---|---|---|---|---|---|
| **1 Quality of Data** | | | | | | | | |
| 1.1 Indicators | | | | | | | | |
| 1.2 Sightings | | | | | | | | |
| 1.3 Courses of Action | | | | | | | | |
| 1.4 Vulnerabilities | | | | | | | | |
| **2 Provider Classification** | | | | | | | | |
| 2.1 Data Feed Provider | | | | | | | | |
| 2.1.1 Provides Original Data | | X | X | | X | | | X |
| 2.1.2 Provides Aggregated Data | | | | | | | | |
| 2.2 Intelligence Platform | | X | X | | X | X | | |
| 2.3 Report Provider | X | X | X | X | X | | X | |
| **3 Licencing Options** | | | | | | | | |
| 3.1 Open (Publicly available) | X | X | X | X | X | X | X | |
| 3.2 Restricted use | | | | | | | | |
| 3.3 Commercial | | | | | | | | |
| 3.4 Information Reuse | | | | | | | | |
| 3.4.1 Commercial use allowed | | | | | | | | |

| Quality Indicator \ Source | Enisa | CERT-EU | National Certs (CERT-FI example) | Framework Nationale per la Cyber Security (Italy) | CERT nationale Italia | Aristotele University of Thessaloniki (AUTH) CERT (Greece)/ Greek School Network CERT | Europol/EC3 | Interpol |
|---|---|---|---|---|---|---|---|---|
| 3.4.2 Academic use allowed | | | | | | | | |
| 3.4.3 Personal use allowed | | | | | | | | |
| 4 Interoperability/Standards | | | | | | | | |
| 4.1 STIX1 | | | | | | | | |
| 4.2 STIX2 | | | | | | | | |
| 2.3 TAXII | | | | | | | | |
| 4.4 OpenIOC | | | | | | | | |
| 4.5 RSS | | X | | | X | | | |
| 4.6 JSON | | | | | | | | |
| 4.7 CSV | | | | | | | | |
| 4.8 Plain Text | | X | X | X | | X | X | X |
| **5 Advanced API** | | | | | | | | |
| 5.1 Filtering based on time | | | | | | | | |
| 5.2 Filtering based on content | | | | | | | | |
| **6 Context applicable content** | | | | | | | | |
| 6.1 Vulnerabilities | | X | X | | X | | | |
| 6.2 Threats | X | X | X | X | X | | X | |
| 6.3 Campaigns | | | | | | | | |
| 6.4 Hashes | | | | | | | | |
| 6.5 Recommendations | X | | X | | | | | |
| 6.6 Incidents (Sightings) | | X | X | X | X | | | X |

| Quality Indicator \ Source | Shadowserver | Abuse.ch | Autoshun | Spamhaus | MISP Platform | GCA | CRiT | Threat Miner | VirusTotal | Hybrid Analysis | Soltra Edge | MalShare | Anomali Staxx | US-Cert AIS | OTX Alienvault | Blocklist | Greensnow Blacklist | Bambenek | BruteForceBlocker | HailATaxii | CVEDetails | Mitre | Nist NVD |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **1 Quality of Data** | | | | | | | | | | | | | | | | | | | | | | | |
| 1.1 Indicators | | X | X | X | X | | X | X | | X | X | X | X | X | X | X | X | X | X | X | | | |
| 1.2 Sightings | | | | | | | | | | | | | | | | | | | | | | | |
| 1.3 Courses of Action | | | | | | | | | | | | | | X | | | | | | | | | |
| 1.4 Vulnerabilities | | | | | | | | | | | | | | | | | | | | | X | X | X |
| **2 Provider Classification** | | | | | | | | | | | | | | | | | | | | | | | |
| 2.1 Data Feed Provider | | X | | X | | | | | | | | | | | | | | X | | | | | |
| 2.1.1 Provides Original Data | X | | X | | | | | | | X | | X | | X | | | X | | X | | | | |
| 2.1.2 Provides Aggregated Data | | | | | | | | X | | | X | | X | X | X | X | | | | X | X | X | |
| 2.2 Intelligence Platform | | | | | X | | X | | | | X | | X | | | | | | | | | | X |
| 2.3 Report Provider | | | | | | | | | | | | | | | | | | | | | | | |
| **3 Licencing Options** | | | | | | | | | | | | | | | | | | | | | | | |
| 3.1 Open (Publicly available) | | X | X | | X | X | X | | | | L | X | X | X | X | X | | X | | X | X | X | X |
| 3.2 Restricted use | X | | | X | | | | | | X | X | | | | | | | | | | | | |
| 3.3 Commercial | | | | | | | | | | | X | | X | | X | | | | | | | | |
| 3.4 Information Reuse | | | | | | | | | | | | | | | | | | | | | | | |
| 3.4.1 Commercial use allowed | | | | | | | | | | | | | | | | | | | | X | | | |
| 3.4.2 Academic use allowed | | | | | | | | | | | | | | | | | | | | | | | |
| 3.4.3 Personal use allowed | | | | | | | | | X | | | | | | | | | | | | | | |
| 4 Interoperability/Standards | | | | | | | | | | | | | | | | | | | | | | | |
| 4.1 STIX1 | | | | | X | | X | | | | X | | | X | X | | | | | X | | | |
| 4.2 STIX2 | | X | | | X | | | | | | | | X | | | | | | | | | | |
| 2.3 TAXII | | | | | | | X | | | | | | X | X | | | | | | X | | | |

| Quality Indicator \ Source | Shadowserver | Abuse.ch | Autoshun | Spamhaus | MISP Platform | GCA | CRiT | Threat Miner | VirusTotal | Hybrid Analysis | Soltra Edge | MalShare | Anomali Staxx | US-Cert AIS | OTX Alienvault | Blocklist | Greensnow Blacklist | Bambenek | BruteForceBlocker | HailATaxii | CVEDetails | Mitre | Nist NVD |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 4.4 OpenIOC | | | | | X | | | | | | | | | | | | | | | | | | |
| 4.5 RSS | | | | | | | | | | | | | | | | | | | | | | | |
| 4.6 JSON | X | | | | X | | | X | | X | | X | | | X | X | | | | | X | | X |
| 4.7 CSV | X | X | X | X | X | | | | | | | | | | X | | | | | | X | X | |
| 4.8 Plain Text | | X | | X | | | | | | | | X | | | | X | X | X | X | | | | |
| **5 Advanced API** | | | | | | | | | | | | | | | | | | | | | | | |
| 5.1 Filtering based on time | | | | | X | | | | | | X | X | X | | | X | | | | X | X | X | X |
| 5.2 Filtering based on content | | | | | X | | | | | | X | | X | | | | | | | | | | |
| **6 Context applicable content** | | | | | | | | | | | | | | | | | | | | | | | |
| 6.1 Vulnerabilities | | | | | X | | | | | | | | | | | | | | | | X | X | X |
| 6.2 Threats | X | X | | X | | | | | | | X | | X | X | | X | | | X | X | | | |
| 6.3 Campains | | | | | | | | | | | X | | | | | | | | | | | | |
| 6.4 Hashes | | | | | X | | X | X | | X | X | X | | | | | | | | | | | |
| 6.5 Recommendations | | | | | X | | | | | | | | | | | | | | | | | | |
| 6.6 Incidents (Sightings) | | | | | | | | | | | | | | | | | | | | | | | |

## Annex 2

Second workshop in Larissa – Kick-off presentation

CS-AWARE CYBERSECURITY

CS-AWARE has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 740723.

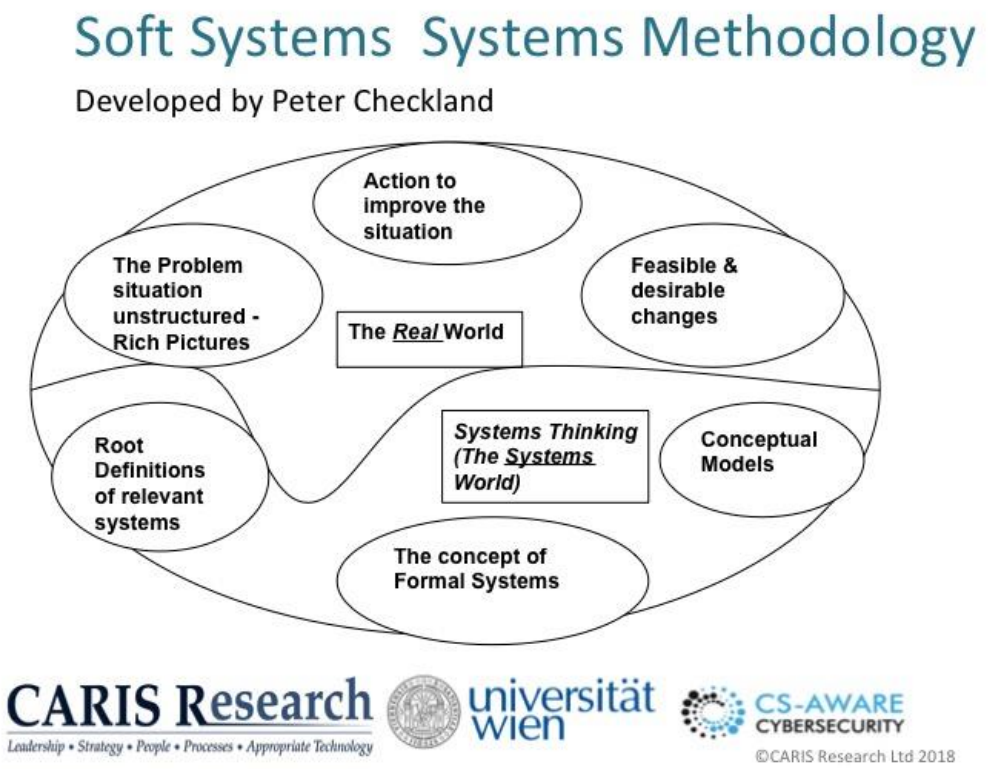
# Soft Systems Methodology

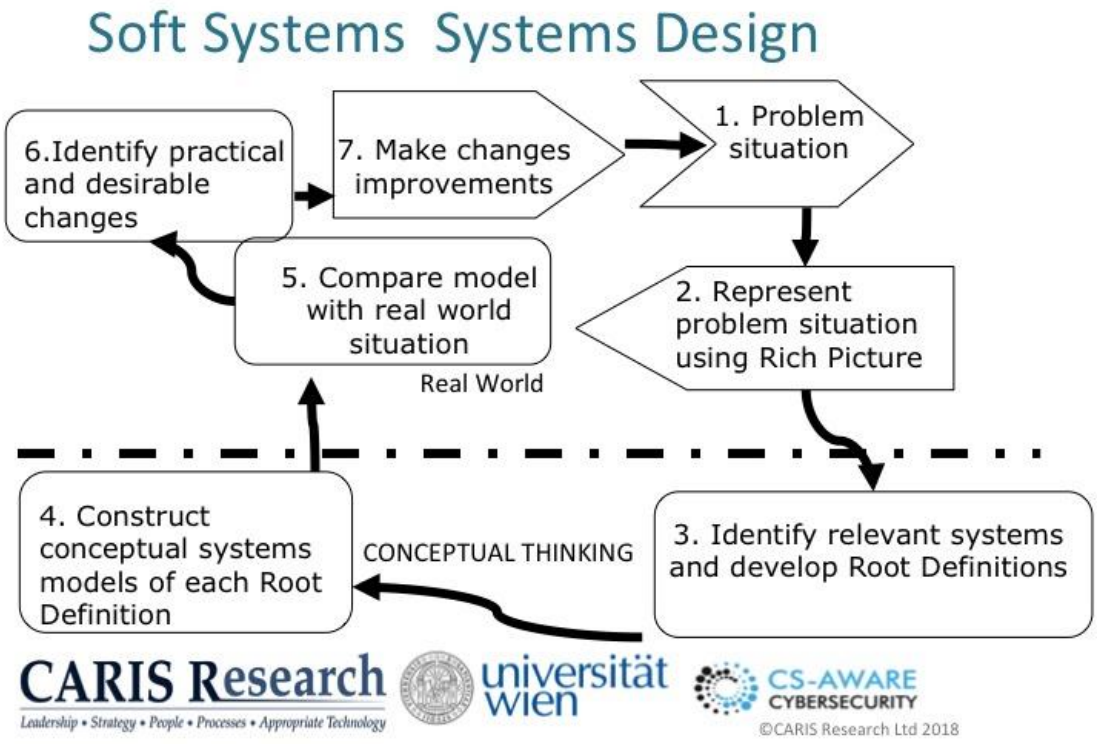
# Root Definitions & Conceptual Models

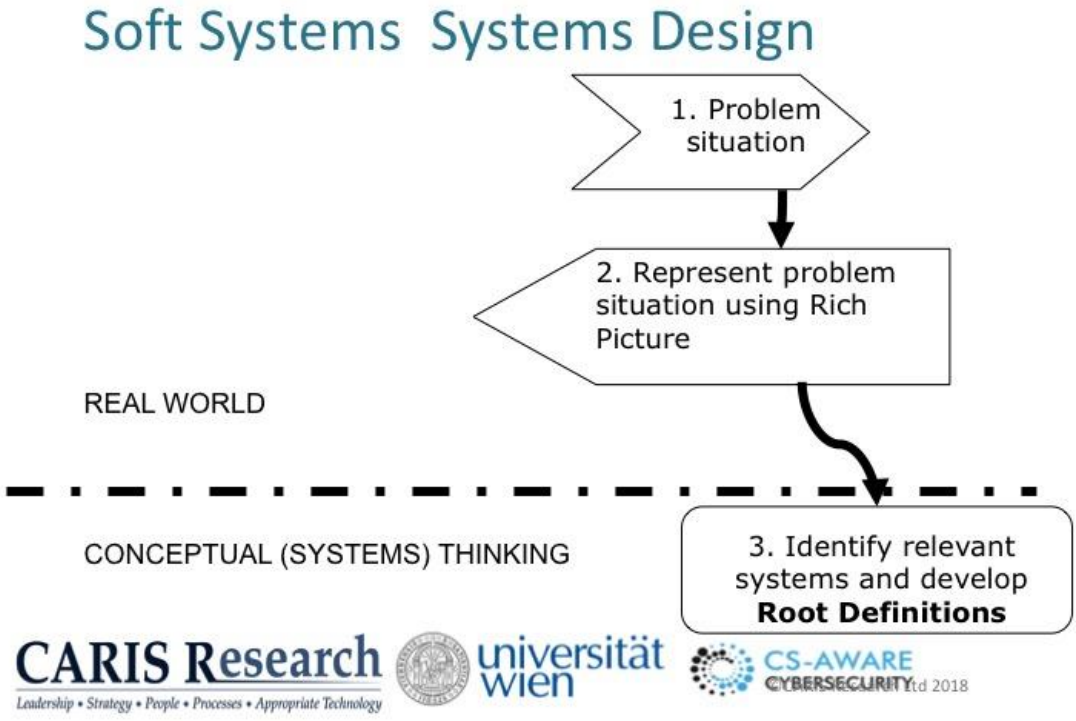
CARIS Research
*Leadership • Strategy • People • Processes • Appropriate Technology*

universität wien

CS-AWARE CYBERSECURITY


Soft Systems Systems Methodology
Developed by Peter Checkland
Action to improve the situation
The Problem situation unstructured - Rich Pictures
Feasible & desirable changes
The Real World
Root Definitions of relevant systems
Systems Thinking (The Systems World)
Conceptual Models
The concept of Formal Systems
CARIS Research
Leadership • Strategy • People • Processes • Appropriate Technology
universität wien
CS-AWARE CYBERSECURITY
©CARIS Research Ltd 2018


Soft Systems Systems Design
6.Identify practical and desirable changes
7. Make changes improvements
1. Problem situation
5. Compare model with real world situation
2. Represent problem situation using Rich Picture
Real World
4. Construct conceptual systems models of each Root Definition
CONCEPTUAL THINKING
3. Identify relevant systems and develop Root Definitions
CARIS Research
Leadership • Strategy • People • Processes • Appropriate Technology
universität wien
CS-AWARE CYBERSECURITY
©CARIS Research Ltd 2018


Soft Systems Systems Design
1. Problem situation
2. Represent problem situation using Rich Picture
REAL WORLD
CONCEPTUAL (SYSTEMS) THINKING
3. Identify relevant systems and develop Root Definitions
CARIS Research
Leadership • Strategy • People • Processes • Appropriate Technology
universität wien
CS-AWARE CYBERSECURITY
© CARIS Research Ltd 2018

# Soft Systems Design

Root Definitions

Root Definitions can be 'activity-based'

Example – A Root Definition of the teaching process at University

A system to enable a University to deliver an effective knowledge transfer system in cooperation with enthusiastic students to achieve and demonstrate accredited levels of understanding in specific subjects leading to a degree in business studies in a supportive, stimulating and friendship-forming environment

CARIS Research
Leadership • Strategy • People • Processes • Appropriate Technology
universität wien
CS-AWARE CYBERSECURITY


# Soft Systems Systems Design

Stage 3 Root Definitions & "CATWOE"

Once the Rich Picture has been constructed, relevant sub-systems are identified and defined using 'Root Definitions' which encapsulate the essence of these systems, the 'whats' (what does it do?) rather than the 'hows' (how does it do it?). The Root Definitions describe the core transformation activities and processes of the system – the conversion of inputs into outputs

CARIS Research
Leadership • Strategy • People • Processes • Appropriate Technology
universität wien
CS-AWARE CYBERSECURITY
©CARIS Research Ltd 2018

# Soft Systems Design

Root Definitions

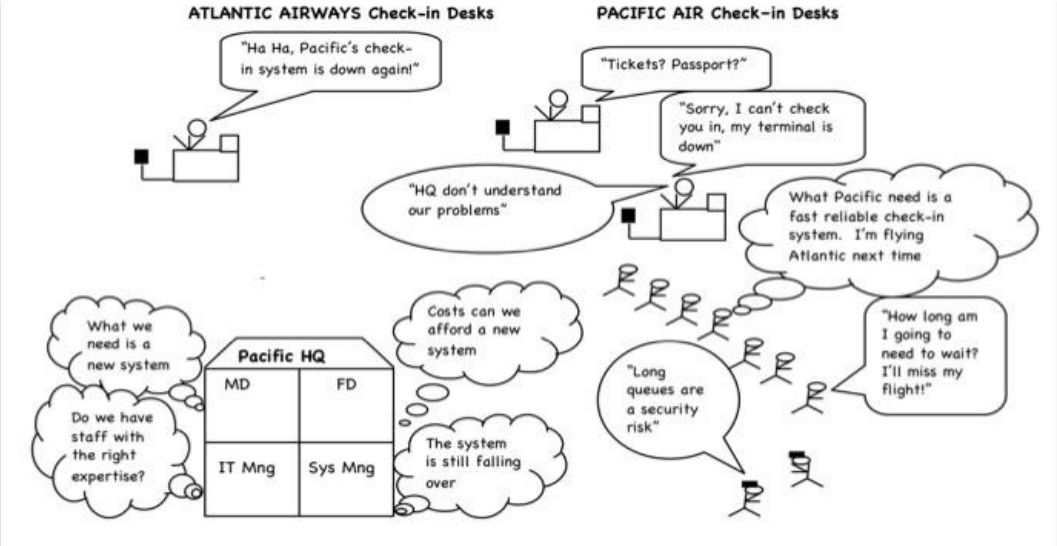
Root Definitions can be 'issue-based'

A system to enable University staff and lecturers to build the confidence of potentially sceptical and often distracted students to enable them to develop the ability to absorb knowledge and demonstrate understanding in order to prepare them for life

CARIS Research
Leadership • Strategy • People • Processes • Appropriate Technology
universität wien
CS-AWARE CYBERSECURITY


# Soft Systems Systems Design

## Stage 2 the problem unstructured




CARIS Research
Leadership • Strategy • People • Processes • Appropriate Technology
universität wien
CS-AWARE CYBERSECURITY

## Soft Systems Systems Design

Stage 3 “Root Definitions”

An example referring to the airline Rich Picture

“An airline owned passenger check-in system that enables passengers to check in their baggage and enables airline staff to issue passengers with boarding cards in a manner that is consistent with the safe and timely operation of the airline’s departure schedules”

CARIS Research
Leadership • Strategy • People • Processes • Appropriate Technology
universität wien
CS-AWARE CYBERSECURITY


## Soft Systems Systems Design

Stage 3 “CATWOE”

Checkland developed the use of a mnemonic “CATWOE” to enable the analyst(s) to ensure that the ‘Root Definitions are complete and accurately represent the problem situation portrayed in the Rich Picture

CARIS Research
Leadership • Strategy • People • Processes • Appropriate Technology
universität wien
CS-AWARE CYBERSECURITY
©CARIS Research Ltd 2018

## Soft Systems Systems Design

### Stage 3 "CATWOE"

**Customers'** - Those who benefit in some form from the system

**Actors**- The people involved

**Transformation** - The development of outputs from inputs

**Weltanschauung**-The 'world view' an holistic overview of both the transformation processes and the problem situation

**Owner**-The person(s) with control

**Environmental constraint** -Physical boundaries, political, economic, ethical or legal issues

CARIS Research Leadership • Strategy • People • Processes • Appropriate Technology universität wien CS-AWARE CYBERSECURITY


## Soft Systems Systems Design

### Stage 3 "CATWOE" – example

**Customers** - The passengers

**Actors**- The airline staff

**Transformation** - Unchecked baggage become checked, passenger tickets supplemented with boarding cards

**Weltanschauung** - The efficacious effective and efficient operation of the Airport and the Airline (it works with minimum waste and meets the expectations of the passengers, the airline and the airport)

**Owner**- The Airline

**Environmental constraint** -Time, safety, security effectiveness (passengers and baggage departing to the same correct destination)

CARIS Research Leadership • Strategy • People • Processes • Appropriate Technology universität wien CS-AWARE CYBERSECURITY

## Soft Systems Systems Design

### Stage 4 Conceptual Models

Once the Root Definition(s) have been constructed and has been compared with the Rich Picture and checked against CATWOE, Conceptual Models can be constructed. The Conceptual Models are formed from the actions stated or implied in the Root Definition(s). Of course, each Rich Picture may be interpreted from quite differing 'world view points'

CARIS Research Leadership • Strategy • People • Processes • Appropriate Technology universität wien CS-AWARE CYBERSECURITY


## Soft Systems Systems Design

### Stage 4 Conceptual Models

Conceptual Models be derived from a **Root Definition** even though knowledge of any 'real-world' version of the activity is lacking

A Conceptual Model is like an **activity sequence diagram**, but is aimed at representing a **conceptual system** as defined by the logic of the Root Definition and not just a set of activities

CARIS Research Leadership • Strategy • People • Processes • Appropriate Technology universität wien CS-AWARE CYBERSECURITY
©CARIS Research Ltd 2018

# Soft Systems Systems Design

## Stage 4 Conceptual Models

A Conceptual Model **is not necessarily** a representation of what exists in reality

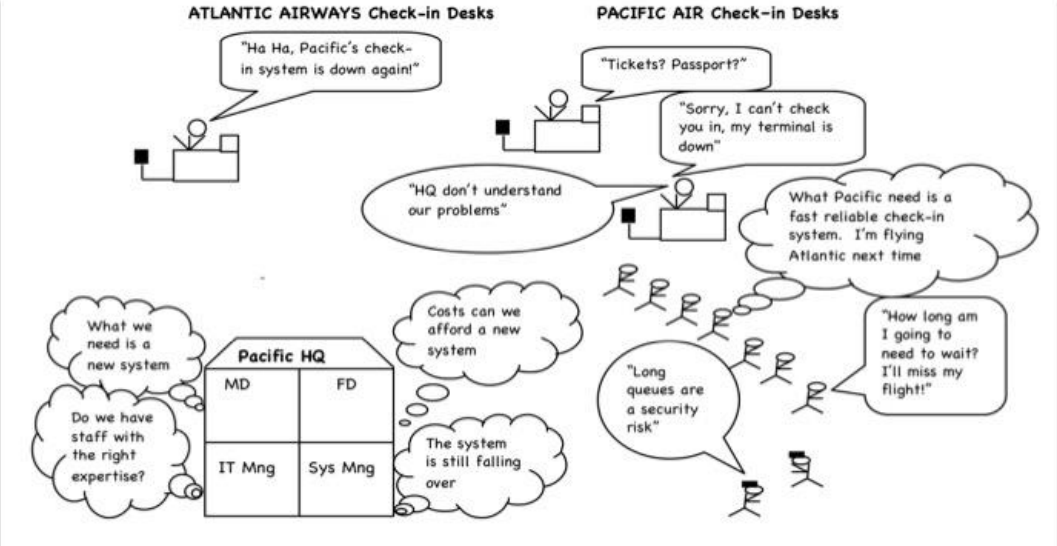
It **is not** a representation of what ought to exist

It should contain only those actions that would have to be carried out, and the order in which they would need to be executed, if the "system" described in the Root Definition is to function

CARIS Research
Leadership • Strategy • People • Processes • Appropriate Technology
universität wien
CS-AWARE CYBERSECURITY


# Soft Systems Systems Design

## Stage 2 the problem unstructured




CARIS Research
Leadership • Strategy • People • Processes • Appropriate Technology
universität wien
CS-AWARE CYBERSECURITY

## Soft Systems Systems Design

Stage 4 Conceptual Models

Conceptual models will differ depending on the view point of the observer

CARIS Research Leadership • Strategy • People • Processes • Appropriate Technology
universität wien
CS-AWARE CYBERSECURITY


## Soft Systems Systems Design

Stage 4 Conceptual Models

Example: **Olympic Games as systems from four viewpoints -**

1. A system to institutionalise a global celebration of sporting prowess and cooperation amongst nation states

or

2. A system to bankrupt major cities on a four-year cycle

CARIS Research Leadership • Strategy • People • Processes • Appropriate Technology
universität wien
CS-AWARE CYBERSECURITY
©CARIS Research Ltd 2018

# Soft Systems Systems Design

## Stage 4 Conceptual Models

Example: **Olympic Games as systems from four viewpoints -**

3. A system to provide inputs into a global capitalist system in which there are limited number of beneficiaries

or

4. A system to allow sports ministers and sports celebrities to extract money from treasuries and taxpayers to develop national sporting infrastructure and competence

CARIS Research
Leadership • Strategy • People • Processes • Appropriate Technology
universität wien
CS-AWARE CYBERSECURITY


# Soft Systems Systems Design

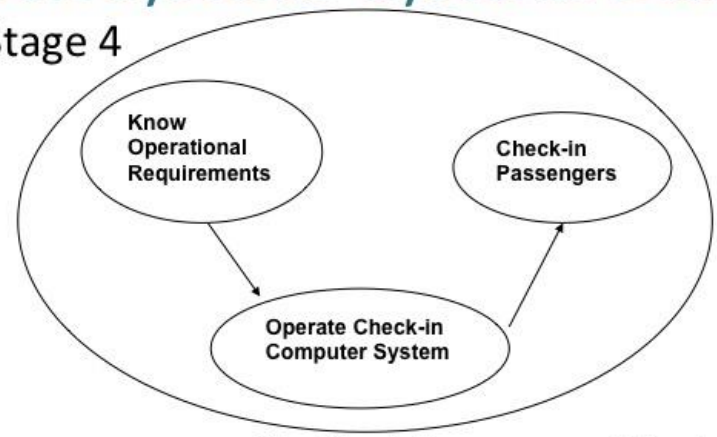
## Stage 4 Conceptual Models

The example of the Conceptual Model in the next slide is from the perspective of the check-in staff. Other perspectives, such as those of Pacific Air's IT manager, would be quite different. When applied in practice, several Conceptual Models would be developed from different view points – as may be the case in this second workshop

CARIS Research
Leadership • Strategy • People • Processes • Appropriate Technology
universität wien
CS-AWARE CYBERSECURITY

## Soft Systems Systems Design

Stage 4




The Check-in process – A Top Level Conceptual Model

CARIS Research Leadership • Strategy • People • Processes • Appropriate Technology
universität wien
CS-AWARE CYBERSECURITY


## Soft Systems Systems Design

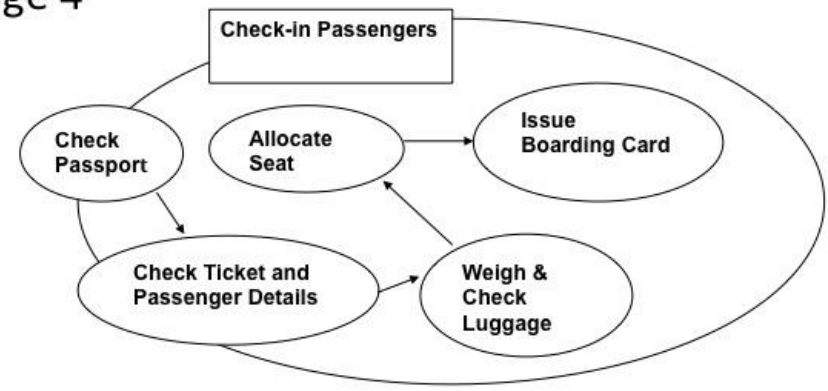
Stage 4 Conceptual Models

Having developed a top level, primary activity Conceptual Model, each of the activities identified are modelled in a second level Conceptual Model

CARIS Research Leadership • Strategy • People • Processes • Appropriate Technology
universität wien
CS-AWARE CYBERSECURITY
©CARIS Research Ltd 2018

## Soft Systems Systems Design

Stage 4




A Second Level Secondary Activity Conceptual Model

CARIS Research Leadership • Strategy • People • Processes • Appropriate Technology universität wien CS-AWARE CYBERSECURITY



## Soft Systems Systems Design

Stage 5

The Conceptual Model(s) are checked against both the Root Definition(s) and the Rich Picture. A good way of performing these checks is to ask three questions: Do the activities exist? Who does them? Why do it that way?

CARIS Research Leadership • Strategy • People • Processes • Appropriate Technology universität wien CS-AWARE CYBERSECURITY

## Soft Systems Systems Design

Stage 5

The analyst(s) need to imagine that the Conceptual Model is actually operating in the real world. They can identify a real process from the Rich Picture, follow its sequence in the Conceptual Model and compare how the sequence would operate in reality. This process can be represented using a chart

CARIS Research Leadership • Strategy • People • Processes • Appropriate Technology universität wien CS-AWARE CYBERSECURITY


## Soft Systems Systems Design

Stage 5

| Activity in Conceptual Model | Present in Real World Situation (Rich Picture) | Comments | Include on Agenda |
|---|---|---|---|
| Check Passport | Yes | Process tasks place independent of check-in computer system | No |
| Check passenger and ticket details | Yes | Dependent upon operation of check-in computer system | Yes |
| Weight and check luggage | Yes | Process tasks place independent of check-in computer system | No |
| Issue boarding card | Yes | Dependent upon operation of check-in computer system | Yes |
| Allocate seat | Yes | Dependent upon operation of check-in computer system | Yes |

Comparison between Conceptual Model, Root Definition and Rich Picture

CARIS Research Leadership • Strategy • People • Processes • Appropriate Technology universität wien CS-AWARE CYBERSECURITY

## Soft Systems Systems Design

Stage 6

Having ascertained that the Conceptual Models are in accord with the Root Definition and Rich Picture, a discussion between the owner and the actors needs to be facilitated by the analyst(s). The objective of the discussion is to identify changes that are both culturally and organizationally desirable and economically and technologically feasible

CARIS Research
Leadership • Strategy • People • Processes • Appropriate Technology
universität wien
CS-AWARE CYBERSECURITY


## Soft Systems Systems Design

Stage 6

In terms of our simple example of an airline check-in system, it is obvious that the key aspect of the problem situation is the poor reliability of the check-in system

CARIS Research
Leadership • Strategy • People • Processes • Appropriate Technology
universität wien
CS-AWARE CYBERSECURITY
©CARIS Research Ltd 2018

## Soft Systems Systems Design

Stage 6

However, as is clear from the Rich Picture, there are a number of competing pressures at Pacific Air's HQ.

The Soft Systems Method enables the analyst(s) to understand the technical problems within the wider context of the problem domain

CARIS Research
Leadership • Strategy • People • Processes • Appropriate Technology
universität wien
CS-AWARE CYBERSECURITY


## Soft Systems Systems Design

Stage 7

The output from stage 6 is applied to the problem situation and may result in changes to procedures, policy, stakeholder attitudes and technology

CARIS Research
Leadership • Strategy • People • Processes • Appropriate Technology
universität wien
CS-AWARE CYBERSECURITY
©CARIS Research Ltd 2018

## Soft Systems Systems Design

Stage 7

By comparing the fit of the real life components with the components which emerge from the Root Definition based Conceptual Model, produce new understanding of:

- Where we are & where we want to be
- What we are doing & and what we should be doing
- How the situation might be improved
  and the best way of getting there which fits with the beliefs of the main participants

CARIS Research
Leadership • Strategy • People • Processes • Appropriate Technology
universität wien
CS-AWARE CYBERSECURITY


## Identify the key Rich Pictures
## Which are they?

Day 1

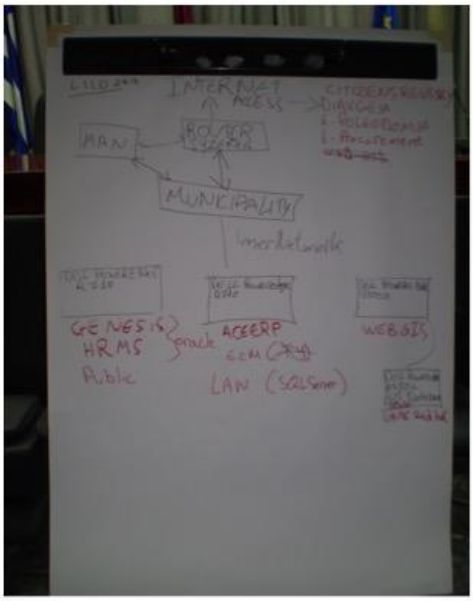
RP1, RP4, RPP7

Day 2

RP1, RP4, RP7

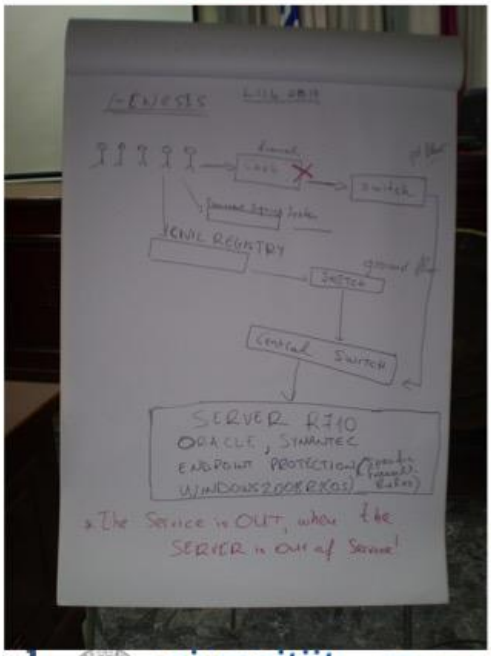
CARIS Research
Leadership • Strategy • People • Processes • Appropriate Technology
universität wien
CS-AWARE CYBERSECURITY
©CARIS Research Ltd 2018

## Day 1 RP1



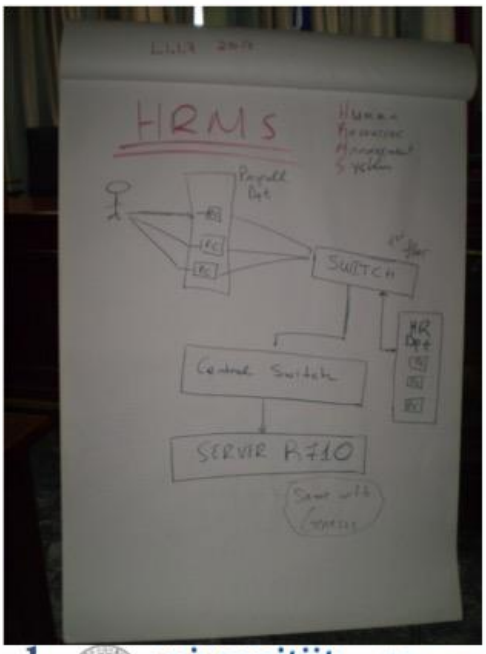

CARIS Research
Leadership • Strategy • People • Processes • Appropriate Technology
universität wien
CS-AWARE CYBERSECURITY


## Day 1 RP4




CARIS Research
Leadership • Strategy • People • Processes • Appropriate Technology
universität wien
CS-AWARE CYBERSECURITY

Day 1 RP7




CARIS Research
Leadership • Strategy • People • Processes • Appropriate Technology
universität wien
CS-AWARE CYBERSECURITY

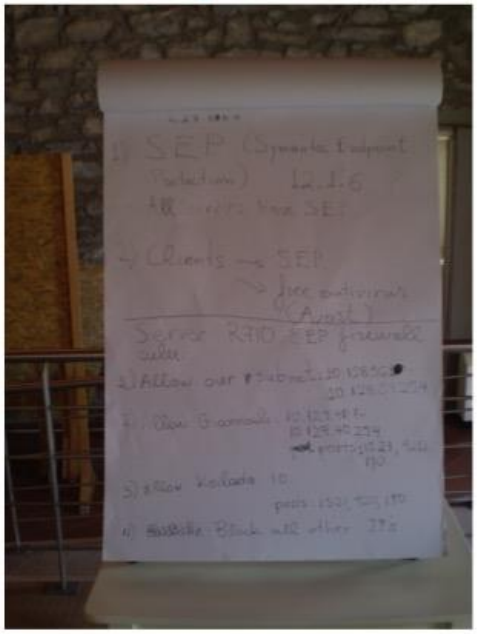

Day 2 RP1


CARIS Research
Leadership • Strategy • People • Processes • Appropriate Technology
universität wien
CS-AWARE CYBERSECURITY

## Day 2 RP4


CARIS Research
Leadership • Strategy • People • Processes • Appropriate Technology
universität wien
CS-AWARE CYBERSECURITY


## Day 2 RP7




CARIS Research
Leadership • Strategy • People • Processes • Appropriate Technology
universität wien
CS-AWARE CYBERSECURITY

## Construct Root Definitions

Root Definitions encapsulate the essence of these systems, the 'whats' (what does it do?) rather than the 'hows' (how does it do it?).

The Root Definitions describe the core transformation activities and processes of the system – the conversion of inputs into outputs

CARIS Research
Leadership • Strategy • People • Processes • Appropriate Technology
universität wien
CS-AWARE CYBERSECURITY


## In this workshop . . . . . .

CARIS Research
Leadership • Strategy • People • Processes • Appropriate Technology
universität wien
CS-AWARE CYBERSECURITY
©CARIS Research Ltd 2018

- Construct Root Definitions and Conceptual Models for the key Rich Pictures

CARIS Research
Leadership • Strategy • People • Processes • Appropriate Technology
universität wien
CS-AWARE CYBERSECURITY


- Compare the emergent Conceptual Models with the representation of Rich Pictures that we have in the GraphingWiki

CARIS Research
Leadership • Strategy • People • Processes • Appropriate Technology
universität wien
CS-AWARE CYBERSECURITY
©CARIS Research Ltd 2018

# Annex 3

## Second workshop in Larissa – Genesis processes CATWOE

A list of the CATWOE analysis results for the 6 identified Genesis processes (subsystems) available to the Municipality of Larissa (ML or DL for short).

### Genesis Subsystem 1: Finance Expenses (a non mission critical subsystem)

Short terms outages of this subsystem do not cause loss of revenue and are recoverable from backup.

| | |
|---|---|
| Customers | Contractors, suppliers, payroll |
| Actors | Staff |
| Transformation | Offer of services or construction or supplies (supplies generating income). This subsystem is used to manage and pay for the construction and maintenance costs of creating and maintaining the City's public buildings and infrastructure. This includes the processing of all day-to-day costs, including energy consumption, personnel costs, vehicle maintenance, procurement and the associated management of contracts. |
| World view | System of managing contracts between DL and customers / clients |
| Owner | DL |
| Environmental constraints | Terms of contract (Law) |

### Genesis Subsystem 2:Finance Revenues (a mission critical subsystem)

Outages my cause loss of revenue and cask flow issues for the Municipality.

| | |
|---|---|
| Customers | Citizens, companies, government |
| Actors | Staff |
| Transformation | Revenue collection in return for the provision of services to citizens - taxes fines etc. The Municipality collects revenue from a wide range of sources; income from the government, rental income from real estate, fees, fines, licenses and local taxes are but some of the examples. This income is used by the Municipality to build and maintain the City's infrastructure, (cleaning, waste collection, public lighting, repairing and managing of communal spaces, new construction such as municipal buildings, pedestrian streets, parking etc.) and to provide other services to the citizens. This subsystem is used to keep track of all aspects of the financial affairs of the City, including billing, collection and debt recovery. |
| World view | System of collecting revenues from citizens and companies to pay for the provisions of municipal services (running costs of the City) |
| Owner | DL |
| Environmental constraints | Time constraints, legal constraints, reliability |

### Genesis Subsystem 3: Documents Archiving (a mission critical subsystem)

Document changes / addition alteration deletions may be possible and this subsystem contains personal data. This subsystem can only be compromised by an insider attack.

| | |
|---|---|
| Customers | Citizens, staff companies, government |
| Actors | Staff |
| Transformation | Inbound and outbound documents received and unique registry number allocated. Every document that comes into or leaves the Municipality receives a unique registry identifier and becomes a record in Genesis. That record has information about the sender, the receiver and the subject of the document. By the beginning of the next year the Municipality will also be keeping a scanned version of original documents, or a digitally signed document. The aim of the new document archiving system is to eliminate paper records and retain only digital information. This will be more easily accessible, but may be vulnerable to attacks. All correspondence will be housed in the documents archiving subsystem of Genesis. Most of the documents and records held in this system contain personal of sensitive data. |
| World view | System keeps detailed logs and categories of inbound and outbound documents |
| Owner | DL |
| Environmental constraints | Deadlines, time (fast, timely response) availability |

### Genesis Subsystem 4: Web Services (a non mission critical subsystem)

| | |
|---|---|
| Customers | Central government |
| Actors | Staff |
| Transformation | DL provides financial data reports (accounting, HR) and uploads them to central government. The municipality makes sure that the relevant central government authorities have access to the financial records and all relevant information held by the Municipality. Such financial data and reports relate to the monitoring of budgets, revenue management, economic balance monitoring and the HR management. |
| World view | The government monitors financial data on a monthly basis in order to keep track of deviations in budget execution. The consequence of being off-track is that funding may be cut. |
| Owner | DL |
| Environmental constraints | Strict deadlines concerning availability |

### Genesis Subsystem 5: Permits

Permits to open businesses and shops in the professional areas of health and hygiene. (a non mission critical subsystem). Some, but not all of the data may be uploaded into the public domain, but some of the information and data may be “personal data” under the terms of the GDPR.

| | |
|---|---|
| Customers | Professionals (Accountant or lawyer) |
| Actors | Staff |
| Transformation | The professionals apply with the proper supporting documents for a permit. The municipality then approves or disapproves) |

| | |
|---|---|
| | Applications to open a shop or start a business in areas like:<br><br>- Selling or cooking and serving of foods or drinks<br>- Funeral homes<br>- Hairdressing salons<br>- Beauty salons (manicure/pedicure/tattoos)<br>- Theatre / cinema<br>- Swimming pools<br>- Hotels<br>- Brothels<br>- Private playgrounds<br>- Internet café<br>- Kiosks<br>- Super markets<br>- Open market/fair (periodic function)<br><br>The subsystem also handles applications from citizens who just want to occupy public space (e.g. with building materials, parking a truck for house moving), have to apply for a permission. The Urban Planning Department checks if the activity of the business is acceptable (for the specific area). The Department of Permissions checks all the supporting documents and registers the application in Genesis (business name, VAT, address, activity, contact person, and whether the application has been approved or denied). The supporting documents are not attached to the Genesis record.The outcome is the approval or the disapproval of the application and monitoring the city's business activity in the area of food and hygiene. |
| World view | City's control over the operation of shops and business premises |
| Owner | DL |
| Environmental constraints | Legislation |

### Genesis Subsystem 6: Decisions of City Council and its committees (a non mission critical subsystem)

The only potential threat is that of Web page defacement.

| | |
|---|---|
| Customers | Citizens |
| Actors | Municipal Councillors, Mayor and staff |
| Transformation | Archiving decisions and uploading to the Internet (Municipality's web site), DIAVGEIA. All the decisions that are taken by the city's committees must be archived in PDF files and uploaded to the Municipality's web site. Additionaly, those among them that have a financial impact are uploaded to DIAVGEIA, in order to have legally enforceable status. DIAVGEIA is conected to one of the central government's data centres and all public entities access it via the internet. |
| World view | Citizens have access to the local administration's decisions |
| Owner | DL |
| Environmental constraints | Legislation, transparency |

# Annex 4

## Second workshop in Larissa – HRMS processes CATWOE

A list of the CATWOE analysis results for the 3 identified HRMS processes (subsystems) available to the Municipality of Larissa (ML or DL for short).

### HRMS Subsystem1: Payroll (a mission critical subsystem)

Staff must be paid and the payments must be accurate and reliable. The subsystem needs to be secure in order to prevent the unauthorised alteration of salaries, data theft of personal information

| | |
|---|---|
| Customers | Staff |
| Actors | Staff |
| Transformation | HRMS calculates salary and unpaid staff gets paid based on the terms of each contract. |
| World view | Staff are paid and deductions for their taxes, social security are made. |
| Owner | DL |
| Environmental constraints | Security. Legislation relating to privacy and sensitive data, time. |

### HRMS Subsystem 2: HR Management (a mission critical subsystem)

| | |
|---|---|
| Customers | Staff |
| Actors | Staff |
| Transformation | Changes to staff data result in changes to staff classification and their position inside DL. |
| World view | DL keeps record of staff's data (education level, working experience, family status, personal data, work experience, disciplinary information) |
| Owner | DL |
| Environmental constraints | Security. Legislation concerning privacy and sensitive data |

### HRMS Subsystem 3: Leave Management (a mission critical subsystem)

| | |
|---|---|
| Customers | Staff |
| Actors | Staff (Only two people have access to leave data) |
| Transformation | Members of staff applies for a leave. Applications are either approved or refused. |
| World view | DL keeps records of all staff leave |
| Owner | DL |
| Environmental constraints | Security. Legislation relating to privacy and sensitive data |

# Annex 5

## Second workshop in Larissa – User Stories

**For Privacy reasons, the gender and further information about the identity of the participants is not revealed.**

### Story 1: Mail for the mayor

One of the tasks of this employee (E1) is to read all mail the mayor receives, which may comprise several hundreds of emails every day. In spite of strict regulations, E1 opened an infected email. This mail had no subject, which could have caused suspicion. After E1 opened the mail, files in each directory on his computer he accessed became inaccessible. The IT-Department was notified, they discovered a type of ransomware that had encrypted all the files in the directories E1 had accessed. The computer was restored in the IT-Department, where all files that were not yet accessed were retrieved, and the system was reinstalled, and the intact files were restored. Infected files could not be retrieved. E1 was initially terrified, feared the computer was lost, but now looks at it as a lesson to more strictly apply the rules for such cases.
*Comment:* The story is interesting because we should be aware there are persons for whom it is a duty to open all email. It also shows that these and other users may be very careful, but still occasional mistakes can slip through. The third interesting point is the role of the IT-Department: they solve the issues, but they also have strict rules. This may lead to users feeling insecure about the IT-issues they still might have.

### Story 2: Inaccessible Network

This user (E2) works with various web-applications as regular part of his work. E2 suddenly was not able to find (on his computer) some other computers and printers on the network. The IT-Department found out this was produced by a worm-virus that caused crashing of computers browsing services. The infection travelled from the web to some user pc across the network to other user-pc's. The IT-Department found a system patch which was able to resolve the issue. It was installed on all computers on the network.
*Comment:* Again, we have a user for whom the work involves accessing various resources on the web that can be sources of compromise: social media, such as Facebook (also applications), chat-applications, google-drive, various web-pages. There is a daily risk. The IT-department is the competent authority to resolve the issues. What happens if they are not available? Is there something else users should know, except following the rules? To be informed of recent issues? This can be a knowledge management issue, with respect to distribution and sharing of knowledge within the IT-department (although they discuss their case on a daily basis), but especially between that department and the other departments. Finally, patches are like pills, they may have side-effects.

### Story 3: The Auto-CAD virus

An officer (E3) from the Urban planning department works with AutoCAD, a design tool. The tool was infected by a well-known virus, that replicates in every folder with AutoCAD files. It can cause files becoming impossible to open and computer crashes, but often nothing happens, so, unlike the previous two cases, it is not always reported. Only after many restarts user E3 reported her problems: I cannot open a file, and my computer restarts. The IT-department easily detected the virus. They not only cleaned the infected machine (which means all the infected files, you have to go through all the folders, this already takes several hours), but also all other machines. But there is

still the danger of users that took home a memory stick with infected files, and will bring this back later, even after a few years.
*Comment:* The virus takes advantage of full-access of some data storage repositories, and replicates in there, and then has possible access to other users of the network repository. External storage devices can also be a source of infection, especially USB-memory sticks that are not only used at the office. Sometimes AutoCAD files have to be exchanged with citizens. Using email or uploading on Google-drive is to be preferred. Scan the USB-stick. Following the rules is the only solution, but we need all people to stick to the rules. Dangers are permanent and a virus may reappear after several years, when an old memory stick re-renters the system.

### Story 4: Opening an email

Of course, all users are careful users, in the departments. Many suspicious mails arrive, from companies, couriers, Nigerian Princes, etc. We know these can be dangerous. But before morning coffee, sometimes it happens that an employee (E4) opens an email and also its attachment. After a while E4 noticed delays in writing to files or folders and with navigation, suggesting a slow connection, and she realised she made a mistake, and felt very guilty about it. She reported to the IT-department nevertheless, and it was noted (informally) this was her second report. The IT-department discovered that there were suspicious records in the registry that led to suspicious execution files in the application data folder. The pc was reset and the problem was solved. User E4 was again reminded of following the strict rules.
*Comment:* Another case of sabotage from an unknown source. Many people have stories like this. Every time the IT department was helpful, and every time the advice is to better follow the rules. Many users may feel guilty.

*The next two stories are provided by people from the IT-department. Can you think about stories that are different, things you were not able to solve so quickly, or imaginary cases of what could happen if people are not careful enough?*

### Story 5: MS17-010

About 1.5 year ago, there was an attack to all Windows machines on the network. One user reported her pc was restarting immediately after initial start-up, and it happened again after two minutes. The IT-officer tried booting with an external source, which seemed to work fine, so there was nothing wrong with the hardware. In the meantime, the same thing happened in another office. Within a few hours ten pc's were affected. Solutions were investigated by looking on social media (external to the municipality) for similar cases. The next day 40 users were affected. Many forums were explored on the network for solutions. What was found was that every infected computer used a (free) antivirus application that was not updated. Other pc's with a different antivirus system had no problems. Windows XP could not handle a specific procedure, (attack through a specific port) which caused the computer to crash and restart. The IT-officers looked for an existing Windows-XP security patch, but Microsoft had stopped supporting this version of Windows. Only much later a patch was released, showing that many other companies suffered from the same attack.
*Comment:* This is an interesting case of security awareness and sharing of information. In addition, there is the use of social media (blogs and forums), relying on information of other security companies. This worked very well. Reports on Facebook of similar cases reveal the possibility that this form of sharing may be widespread.

### Story 6: Hiring Temporary support

In our municipality we pretty much know each other, people have permanent working contracts that helped to survive the last 8 years of depression. However, during that same period there were also

many new colleagues coming and going on temporary contracts (between 2 and 8 months). This increases the tension related to trust and openness of networked information and services. It is possible in many cases to retrieve database information in a readable excel format. It is hard to monitor the behaviour of people we do not know very well, who work with some client computer.
*Comment*: In every networked system, people rely on each other and trust evolves over time about the reliability of people in maintaining the strict rules of cybersecurity. With more temporary contracts, it is more difficult to develop such trust, and the dangers for sabotage and theft increase. How to deal with such conditions? Give some people less permissions? It shows how much cybersecurity is a matter of user behaviour.

# Annex 6

## Third workshop in Rome – SUET process CATWOE

### SUET Subsystem 1: Drafting and Submission

| | |
|---|---|
| Customers | Citizen |
| Actors | Technician/Citizen/Payment System |
| Transformation | Request - Instance |
| World view | Planning APP |
| Owner | Rome Municipality |
| Environmental constraints | Italian Laws and Regulation on Urban Buildings |

**Description of the process:**

SUET allows, in accordance with the latest urban regulations, the digital management of end-to-end process for filling, submission and verification activities relating to building procedures (CIL - Comunicazione Inizio Lavori, CILA - Comunicazione Inizio Lavori Asseverata, SCIA - Segnalazione Certificata Inizio Attività, PDC - Permesso di Costruire).
From a workflow point of view the SUET application can be divided in two parts:

- the Front-End side;
- the Back-End side.

The main actors of the front-end side are Technicians and Citizens. Both must be registered within the Roma Capitale Portal to access the application.
Technicians prepare the building request by filling all the required fields and uploading all the required documents (technical and administrative documents). They must indicate within the request the owners of the request (Citizens) and all the other technicians involved within the building process. Once the request is completed, the system produces a document called “Technical Report” that is digitally signed by the Professional before to be shared with the owner (Citizen). At this point, the system notifies to the owner (through a mail) that the request is ready to be submitted.
The owner accesses the SUET, verifies the request and uploads the payment receipt before to submit the building request. To date there isn’t an integration between the SUET end the Roma Capitale Payment System. When the request is submitted the SUET calls the Roma Capitale Documental System to generate a protocol that become the Building Instance unique identifier. The authentication process is the same for both internal and external users. In both cases, access requires a password.

### SUET Subsystem 2: Verification and Approval

| | |
|---|---|
| Customers | Citizen |
| Actors | Employees/Managers/Citizen |
| Transformation | Instance – Building Permit/Deny |
| World view | Application for verification and approval of building permits |
| Owner | Rome Municipality |
| Environmental constraints | Italian Laws and Constraints |

**Description of the process:**

A. VERIFICATION
- a. Administrative check
  - i. Documentation Check (technical check)
  - ii. Payment Check (administrative check)
  - iii. Law Check
- b. Technical check
  - i. Volumes, Areas
  - ii. Technical Laws

B. APPROVAL
- a. Check OK or KO

The main actors of the back-end side are employees and managers. Both must be registered within the Roma Capitale Portal to access the application.
The employees must verify the respect of administrative and technical urban constraints and they must express a general opinion on the building instance. They perform a check both on documents and payments and if the Instance required additional information they can ask to the Professional/Owner to integrate it. Managers have the final responsibility to approve or reject the Instance; if they approve the Instance, in some cases (depends on the kind of Instance) the building permit is generated. Otherwise the permit is denied.

### SUET Subsystem 3: Employees/Managers Enablement

| | |
|---|---|
| Customers | Employees/Managers |
| Actors | Employees/Managers/ICT Department/Local Municipalities |
| Transformation | From official letter to role-based enablement |
| World view | Application |
| Owner | Rome Municipality |
| Environmental constraints | Office Organization |

The Technicians, the Citizens, the Employees and the Managers must be registered within the Roma Capitale Portal to access the SUET application. Moreover, the Technicians must be authorized by the Urban Planning Department to draft the request.
The Technicians access the SUET application as Citizens and they submitted the request to be enabled to operate as a Professional. Once the request has been received, the Urban Planning Department check that the Technicians are correctly listed within the Italian professional register of Architects, Engineer and so on and it decide if accept or deny the request. The same Technician can operate within the SUET using more qualifications (one for each request has been submitted).
The employees that can operate within the SUET are divided in simple employees and managers, the profile to use is indicated from the Local Municipalities to the ICT Department through an official letter. The ICT Department insert the association employee/profile within the SUET Database.

# Annex 7

## Third workshop in Rome – IAM process CATWOE

### IAM Subysstem 1: Registration

| | |
|---|---|
| Customers | Citizens/Employees |
| Actors | Internal employees of "internet services" – Call Center "060606" – Certification Authority SPID/CNS |
| Transformation | rom user's data to User credentials |
| World view | Registration System |
| Owner | City/Municipality |
| Environmental constraints | Check on passport/Identity of user – Citizen of Italy (or italian tax payer) |

The registration procedure is a Registration System (world view) that allows the user to be recognized whenever he/she will try to access and to use the internal/external (depending on the role of the user) services, including the ones that are not publicly accessible, provided by Roma Capitale. The procedure is available for two kind of customers: Italian citizens and employees of Roma Capitale.
It is managed by (actors) the internal employees of the "internet services", by the employees of the "060606" call center service and through the use of identifications system (SPID, CNS) acting as certification authorities. The aim of the registration procedure is to collect the user's data used for activation procedure and to provide back the credentials to access the internal/external services (transformation). The principal environment constraints of the registration system are based on two main controls: the manual check of the official identification document (identity card, passport,..) of the registering user and controls on Italian nationality or if the user pay taxes in Italy. The overall procedure is owned and managed by the municipality (owner). In the authentication process, the user's credentials are checked and the system either recognises the user or not. If the user is recognised as a legitimate user, the system grants the correct and appropriate access rights to the user.

### IAM Subsystem 2: Authentication

| | |
|---|---|
| Customers | Citizens/Employees |
| Actors | SPID / CNS (External Citizens) – Username/password (Internal Employees / Citizens) |
| Transformation | Credentials to Authenticated Sessions |
| World view | Authentication System |
| Owner | Certification Authority: CNS, Identity provider: SPID, Municipality:Username/password |
| Environmental constraints | Check on wrong credentials - Check on validity of credentials |

The authentication procedure is an Authentication System (world view) that allows the registered users to access and to use the external/internal services (depending on the role of the user), including the ones that are not publicly accessible. This procedure as well is available for two kind of customers: Italian citizens and employees of Roma Capitale.
It is managed basically by (actors) two identification systems depending on the role of the user accessing the services. The citizen-user can access to all the public and private external applications

provided by Roma Capitale using SPID and CNS. The employee-user can access through an internal login system which allows him/her to access all the private internal services (all those services that are related to the relationship between the employee and the municipality).
The Authentication System basically checks the credentials of the user accessing the online services and, having the control procedure a positive outcome, provides the users with an authenticated session in order to navigate through the applications (transformation). As environmental constraints the authentication procedure carries on a double check on the credentials, both on the correctness and on the validity. The correctness is related to the cross-control of the pair username/password of a user. The validity is a further control which identify if the password is expired. The authentication procedure is managed by two different entities depending on the role of the user authenticating. The citizen-user authentication is handled by the identity providers (SPID, CNS), while the employee-user authentication is handled by the municipality (owner).

### IAM Subsystem 3: Authorization

| | |
|---|---|
| Customers | Citizens/Employees |
| Actors | Access Management System / identity manager |
| Transformation | From Authenticated to service access |
| World view | The proper user has access to the proper service |
| Owner | IAM System or the municipality |
| Environmental constraints | to have access rights |

The authorization procedure is a system (world view) that controls whether the user session is authorized to access the use of external / internal services (based on the user's role), including those that are not accessible to the public. This procedure is also available for two types of customers: Italian citizens and Roma Capitale employees.
It is fundamentally managed by (actors) an access management system based on the role of the user accessing the services. The city user can access through the use of SPID and CNS and can therefore access all public and private external applications provided by Roma Capitale. The user-employee can access through an internal access system that allows him to access all the internal private services (all those services related to the relationship between the employee and the municipality).
The authorization system essentially controls whether an authenticated session has the characteristics to access that service, it provides users with access to the service by checking the session (transformation). As environmental constraints, the authorization procedure gives access to services only if a session exceeds the constraints of the access policies. The user characteristics are managed by the identity manager system (owner).

### IAM Subsystem 4: User Management

| | |
|---|---|
| Customers | Citizens/Employees |
| Actors | BackOffice Operator, idm system, Citizens , employees |
| Transformation | From virtual identity data to modified virtual identity data |
| World view | system to modify userdata |
| Owner | Municipality / IDM System |
| Environmental constraints | The rights of the operator (Employee, based on municipal districts) |

The user management procedure is a system of (world view) that controls the user's life cycle. This procedure is also available for two types of customers: Italian citizens and Roma Capitale employees.
It is fundamentally managed by (actors) backoffice operators, system of identity managers, citizens and employees. The management is based on the role of the user accessing the services. Operators or users themselves, through specific services, can modify their own (in the case of the citizen / employee) or other information. The system, through specific tasks, carries out autonomous interactions: for example the obligation to change the password. The input system receives user data to modify them (transformation). As environmental constraints, only the identity manager system has the possibility to implement the changes. The procedure for managing users to authorize access to services only if a session exceeds the constraints of access policies. Based on specific policies, the system controls who can change, the scope with which it can carry out the modification and what to change (owner).

# Annex 8

## Second user workshop in Rome – User stories

**For Privacy reasons, the gender and further information about the identity of the participants is not revealed.**

### Story 1: Phishing

An email (from an external user) contained the image of the opening page of their municipal web account, asking for user credentials for verification purposes. A few dozen of users provided their credentials to a fake URL. After a few hours Internet Services (The IT-dept.) was aware of the danger and they acted to neutralise the danger (localise the infected pc's from system logs, block their accounts, reset passwords, blacklist the fake URL). It is unknown what happened with the stolen information, nor what was the perception of the users who were compromised. The attitude seems to be that this can happen to anyone. Also, there was no follow-up by Internet Services. So, it may well happen again. This especially true since it is easy to make up an email address if you know the name of an employee of the municipality.

*Comment:* This story was produced by a group of system administrators who imagined themselves as users. Therefore, it is hard to assume the full user viewpoint, and this analysis will be incomplete. This story is a classical phishing case, and some users were aware of the danger immediately. Others were not, but it is unclear what numbers they represent. It appears there was no follow-up, as when other users are immediately informed of this danger, or later when all users are informed about recent dangers. We do now know to what extent user regulation concerning suspicious emails are spread amongst the employees of the municipality. We might have to deal with serious knowledge management problems that will not be resolved with a better virus detection system, in addition it raises questions about what the awareness services of such a system need to accomplish.

### Story 2: Fake News

In the news media it was written that the personal identity of many citizens that registered on the portal was stolen. This included the Mayor herself! The Internet Services were alerted by a journalist about this news. After a lot of time spent on inspecting the system and the log files, it could be affirmed that the news was fake, and there had been no stealing of identities.

*Comment:* amongst the many dangers, the occurrence of fake news, or manipulated news is a more recent one. This is hard to handle by traditional virus scanners because it involves confirmation that there is nothing wrong with the system. It only works when the system is sure of itself: I detected nothing wrong! As we will learn later, the system in Roma cannot be certain, because its updates are erratic. Another option would be the possibility to question the system, to ask the system questions about a general class of certain symptoms that have not previously been diagnosed as dangerous. We may wonder what the interest of such fake news attempts is, probably disrupting the image of the town municipality.

### Story 3: Forbidden websites

This user group generated a story about the restrictions to visit websites. This particular user works at a department responsible for manging European contracts. The problem that is frustrating our user, and probably many others, is that some websites from the EU are forbidden by system administration. On the other hand, many websites that are more dangerous are open for all, such as Zalando or Facebook. The procedure for employees is for the head of the department to write an official request for access to certain websites by certain people. This helps, but only for the people who have been listed in the request. For some people, phone calls can be a solution too. The issue is

that some websites that can be dangerous are not closed for the employees of the municipality, while some websites who are well protected, cannot be visited. Even worse, the main website from the municipality is rated unsafe by most virus trackers, because it is not updated. All of this is interpreted as erratic by our user: is there any policy behind this?
*Comment:* The issue seems to be that the policy behind allowing or restricting websites within the municipality is unclear, and probably erratic, in the sense that it may be the result of many policies operating at the same time, including individual decisions. As a consequence, some things are allowed and some things are not allowed. For the user, this is highly unsatisfactory and confirms a lack of trust, in addition to searching for individual solutions rather than for those that relate policy issues in general. There clearly is a transparency problem for the IT-Department AND for individual users.

### Story 4: Password reset

This is the classical story about somebody who called the IT-Department to reset his password, because he forgot what it was. The IT-employee asked for the user's personal name (instead of for some codes only known to this user), which was Mario Rossi. The password for Mario Rossi was then reset. Unfortunately, it turned out that there were 3 Mario Rossi's working for the municipality (it is a very common name and there are more than 20.000 employees), and the wrong Mario Rossi's password was reset. This only appeared when Mario Rossi I called again telling he could still not enter his email. This was now settled, but then there still was the issue of Mario Rossi 2, whose password was also reset, by mistake. This appeared to be an employee who had retired two months ago. This revealed the problem that when people leave, the IT-department is not informed.
*Comment:* This is another problem for the IT-department, that their own employees do not always follow procedures. In addition, the question is how to solve the problem what happens when someone leaves. Again, we do not know what the user experienced, as this story was produced by the system administrator group.

### Story 5: Web conferencing

A large municipality can save a lot of time and money when its employees do not have to travel to meet their colleagues at other places, or even abroad, but instead can use web conferencing, such as skype or WebEx. This is formally not allowed by this municipality. Informally however, employees can use their Phone on the G4 network, or they can work from home. This is what most people do. There is a problem when files on personal laptops are compromised and transferred, or when files from compromised USB-sticks are transferred through the conferencing app.
*Comment:* This is a similar story as story 3, and it adds to the lack of trust in IT-policy making. There was no sign of understanding by this user why web conferencing was forbidden by the municipality. On the one hand, many users from other public organisations may recognise this issue. On the other hand, more transparency of policy rules and more interest in user perspectives may well contribute to less issues and greater trust.

### Story 6: Patching

This story confirms there is no policy for patching and updating from the side of the IT-department, and this is not seriously considered by management. It is not verified if users use the latest versions of software, and all updates and patches are installed. There is no test environment operative. The management says there is a lack of money.
*Comment:* At the management level there seems to be a clear lack of attention to security updates and patches. Will awareness in this respect help anything?