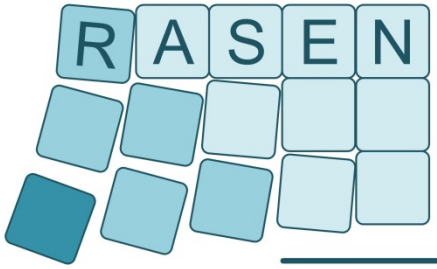

Compositional Risk Assessment and Security Testing of Networked Systems

Deliverable D2.1.1

Use Case Scenarios Definition

Project title:	RASEN
Project number:	316853
Call identifier:	FP7-ICT-2011-8
Objective:	ICT-8-1.4 Trustworthy ICT
Funding scheme:	STREP – Small or medium scale focused research project

Work package:	WP2
Deliverable number:	D2.1.1
Nature of deliverable:	Report
Dissemination level:	PU
Internal version number:	1.0
Contractual delivery date:	2013-01-31
Actual delivery date:	2013-01-31
Responsible partner:	Software AG

Contributors

Editor(s)	Frank Werner (Software AG)
Contributor(s)	Albert Zenkoff (Software AG), Arthur Molnar (Info World), Erlend Eilertsen (EVRY)
Quality assuror(s)	Ketil Stølen (SINTEF), Jürgen Großmann (FOKUS), Fredrik Seehusen (SINTEF)

Version history

Version	Date	Description
0.1	12-11-2012	Initial draft of TOC and preliminary structure of use case template (SAG)
0.2	12-11-2012	Revision of TOC and to dos (SAG, IW)
0.3	16-11-2012	Alignment of Use Case Scenarios
0.3.1	28-11-2012	Redesign of Use-Case Template
0.3.2	07-12-2012	Revision of Use-Case Template
0.4	20-12-2012	Integration of Chapter 6 and 7
0.5	21-12-2012	Document ready for internal review
0.6	10-01-2013	Incorporating review from FOKUS
0.7	28-01-2013	Incorporating review from SINTEF and finalizing for last internal comments
0.8	29-01-2013	Final fixes and preparation for final check
1.0	31-01-2013	Final quality check and polishing

Abstract

The overall objective of RASEN WP2 is to identify use case scenarios contributed by the partners in the project, analyze them regarding their requirements, and finally evaluate the case studies on software developed within the project.

The case studies provided address different problems scenarios and provide input for R&D of subsequent tasks and for evaluation of tools and method in the technical work packages.

This document describes case studies provided by project partners for the RASEN project. Selected scenarios are chosen from the fields of business software, medical information systems, and the financial sector and will establish the basis for further analysis and requirements definition in the following tasks.

Keywords

case study, industry domains, IT security requirements, security risk assessment, business software, medical information systems, financial sector

Executive Summary

The overall objective of RASEN WP2 is to provide use cases in which the R&D results of the RASEN project can be evaluated and exploited. The purpose of this document is to give an overview of the relevant use case scenarios and to show the expected improvements for the use case providers in RASEN.

The tasks for WP2 are closely related to WP3, 4 and 5. WP2 is split into three tasks: T2.1, T2.2 and T2.3.

- T2.1: Use case scenario definition – identification and description of use case scenarios from the use case providers that are of relevance to the RASEN project.
- T2.2: Use case requirements definition – Extraction of requirements from the use cases to the R&DE work packages.
- T2.3: Use case evaluation – Evaluation of the R&D results of the RASEN project in light of the use case requirements.

This document is related to task T2.1 and delivers a description of use cases provided by project partners from different industries which are considered within the RASEN project, taking into account existing security assessment and testing infrastructures from the partners. The use cases will encompass scenarios from the domain of business software developers, the medical information domain, and the financial domain.

In this context this work has a preparatory character since it defines use cases, including a description of the systems that will be targeted by the case studies and a description of the current processes for security testing which will be re-used in the up-following tasks.

Table of contents

TABLE OF CONTENTS **5**

1 INTRODUCTION **7**

1.1 APPROACH FOR WORK PACKAGE 7

2 OVERVIEW OF CASE STUDIES **9**

2.1 OVERVIEW OF USE CASES 9
2.2 USE CASE TEMPLATE 9
2.2.1 Stakeholders 10

3 CASE STUDY: SOFTWARE AG **12**

3.1 INDUSTRY SECTOR: ENTERPRISE BUSINESS SOFTWARE 12
3.1.1 Software Portfolio 12
3.1.1.1 TERRACOTTA 13
3.1.1.2 ARIS 13
3.1.1.3 WEBMETHODS 13
3.1.1.4 ADABAS 13
3.1.1.5 NATURAL 13
3.1.2 Technical Aspects and Customer Requirements 13
3.1.2.1 Key Software Requirements 14
3.1.3 Reference standards of importance 14
3.1.3.1 Common Criteria for Information Technology Security Evaluation (ISO 15408) 14
3.1.3.2 NIST Publications: US Government requirements 15
3.2 RELEVANCE TO RASEN 16
3.2.1 Actors 16
3.2.2 Targeted Software Systems 17
3.3 USE CASE DESCRIPTIONS 17
3.3.1 Description of Current Processes 17
3.3.1.1 Use-Case Scenario I: Enterprise Software Production Process 18
3.3.2 Key Figures in the Security Testing Process 18
3.3.3 Security Testing involved in Software Production Process 19
3.3.4 Expectations from RASEN 21
3.3.4.1 Risk Analysis of newly implemented Features 21
3.3.4.2 Risk selection and mitigation 21
3.3.4.3 Compositional Risk Tracking 22
3.3.4.4 Product Prioritization and Risk Rating 22

4 CASE STUDY: INFO WORLD **23**

4.1 INDUSTRY SECTOR: MEDICAL INFORMATICS DOMAIN 23
4.1.1 Technical and Legal Aspects 23
4.1.2 Actors 25
4.2 RELEVANCE TO RASEN 26
4.2.1 Actors 26
4.2.2 Targeted Software Systems 26
4.2.2.1 Admission, Discharge, Transfer Service (ADT) 27
4.2.2.2 Entity Identification Service (EIS) 27
4.2.2.3 Retrieve Locate and Update Service (RLUS) 28
4.2.2.4 Enterprise Vocabulary Service (EVS) 28
4.2.2.5 Security Services 29
4.3 USE CASES DESCRIPTION 32
4.3.1 Targeted Processes within Info World 32
4.3.1.1 Development of New Features 32
4.3.1.2 Security Testing 36
4.3.2 Expectations from RASEN 38

5 CASE STUDY: EVRY **40**

5.1 INDUSTRY SECTOR: FINANCIAL DOMAIN 40

5.1.1 Technical and Legal Aspects 41
5.1.2 Actors 42
5.2 RELEVANCE TO RASEN 42
5.2.1 Resources involved 42
5.2.2 Targeted software system 42
5.2.2.1 Private Net Bank 42
5.2.2.2 Mobile bank 43
5.2.2.3 Tablet bank 43
5.3 USE CASE DESCRIPTION 43
5.3.1 Security testing 43
5.3.1.1 Test and development methodology 45

6 A UNIFIED VIEW OF THE USE CASES 46

6.1 THE CASE STUDY PROVIDERS 46
6.2 RISK ISSUES 47
6.3 LEGAL ISSUES 47
6.4 SECURITY ISSUES 48
6.5 USE CASES DISCUSSION 49

7 CONCLUSION 50

REFERENCES 53

APPENDIX A: USE-CASE SCENARIO TEMPLATE 54

1 Introduction

The main objective of this deliverable (D2.1) is to identify the use case scenarios contributed by partners for evaluating demonstrating the advantages and the benefits of the approach targeted by the RASEN project. Accordingly, three case studies are illustrated from different domains.

What is very specific is that each of these case studies addresses different problems and aspects, providing a possible range of scenarios. Additionally by providing input for the R&D of subsequent tasks and for the successful evaluation of tools and methods developed in the technical work packages, it is prerequisite to clearly identify similarities and overlaps during the assessment of the use cases.

In detail, the following industry domains are addressed within the project:

- Software development of business, process, and enterprise related solution provided by Software AG
- IT solutions and products found in the medical and health sector addressed by Info World
- Software and IT Systems developed for the financial domain by EVRY

To obtain a mutual understanding about the intended use scenarios and in order to make them comparable, a concise structure is proposed in a way that each case study follows the same schema for the presentation of its content. The schema entails a detailed use case description, the use of a use-case template for structuring the detailed information, putting a special emphasis on RASEN-relevant aspects. As an initial step it is therefore relevant to describe the current work processes of the case study providers relevant to RASEN. The RASEN results can later on be applied to current work processes, which, in combination with the expected improvements, serve as a good starting point for future work.

1.1 Approach for Work Package

The tasks of WP2[1] (c.f. Figure 1) are tightly related to research oriented activities contained in work packages 3, 4 and 5. The first activity of WP2 consists of identifying relevant use cases originating from different industrial sectors that will be used to guide and evaluate the results of the RASEN project. The three case study providing partners develop highly-complex networked systems that are widely used and have stringent security and privacy requirements. Therefore, task T2.1 undertakes the analysis of the partner use cases and identifies similarities and differences between existing processes in each organization.

Task T2.2 is used to extract requirements for the other scientific work packages from the provided case studies. Concrete use case processes are to be abstracted so they take on a more general nature, ensuring the wide applicability of the undertaken research.

The final task of WP2 is task T2.3. Task 2.3 is the most complex undertaking of WP2 and its implementation is planned over two iterations. After the first research phase, research and technology partners will provide the results to the case study providers and will assist them in implementing the new tools and methodologies within their processes. The case study providers will then report the experience of employing the first phase results to the research and technology providers, which will guide the second R&D phase of RASEN. The second iteration will be similar to the first, only that its results will guide the R&D phase 3 of the project.

[1] Work Package 2

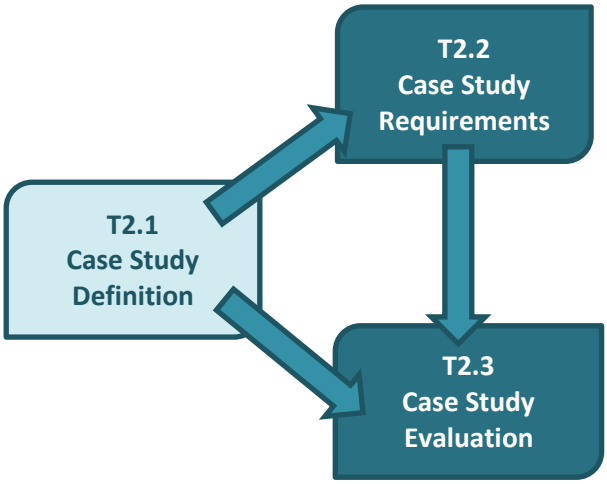

Figure 1 – Overview and dependability of tasks within Work Package 2

As WP2 provides relevant information about real-world organizations that are directly interested in advancing the state of the art, the tasks that comprise it are relevant to all technical work packages, namely WP3, WP4 and WP5. These three work packages must take input from the use cases defined in WP2 and then consult the results obtained by the case study providing organizations when employing the provided methodologies and software in order to guide RASEN research in the direction of maximizing the benefit for the end-users.

2 Overview of Case Studies

This chapter provides an overview of the RASEN use cases and the key concepts underlying the use cases. The use case descriptions capture actors, a description and a short descriptive view of the underlying process.

Based on this a further exploration of the prevailing situations at the partner's domains is feasible. By the use of a well-structured template-style approach, different use cases are collated and displayed in a comparable way.

For the remainder of this deliverable we prefer to distinguish between *case studies and use case scenarios* or just *use cases* for short. A case study is considered as the contribution of a case study provider whereas a use case is considered to be a part of a case study.

2.1 Overview of Use Cases

The provided case studies try to collect relevant information from the industry domain and structure them in a way which makes them comparable and accessible for future tasks. Having the overall focus of the RASEN project in mind, this deliverable tried to foster the application of the RASEN methodology. For the part of the use cases this is done by collecting required information and subsequently creating the full picture of the scenarios.

A short summary of the established and described use cases is found in Table 1.

Use Case ID	Name	Industry Domain	Issues/target	Reference
SAG_S_1	Enterprise Software Production Process	Business	Security	Table 4
IW_RSL_1	New Feature Implementation Process	Medical	Risk assessment, Security and legal	Table 5
IW_SL_2	Security Testing Process	Medical	Security and legal	Table 6
EVRY_SL_1	Security Testing Process	Financial	Security and legal	Table 7
EVRY_SL_2	Development Methodology	Financial	Security and legal	Table 8

Table 1 – Overview of Use Cases

2.2 Use Case Template

To provide a uniform use case description, all use cases are summarized with the help of a *use case template*. The detailed structure of this template is shown in Appendix A: Use-Case Scenario Template and is designed to be descriptive enough to function as a basis for identification of the upcoming requirement analysis in the next task of WP2. Within the use case template, requirements are expressed partly in narrative, natural language where a descriptive idea of the situation is necessary. In some cases e.g., where either processes of subsequent situations are considered, an enumerated listing is used.

A detailed explanation of the use case template developed within this task is depicted in Appendix A: Use-Case Scenario Template. Regarding the information, the following information is considered to be very relevant:

- use case name
- category of the use case
- brief description of the situation
- Purpose and requirements of the described task
- Primary stakeholders

- A more detailed narrative description of the situation
- A structure and formalized use-case template

In the following the use cases of the different industry domains are clustered by the industry domain of the partner. The following industry domains are covered with their corresponding abbreviation in parenthesis:

- software production for enterprise and business applications (Business)
- IT solutions and products in the area of health care and medical systems (Medical)
- banking and financial solutions (Financial)

2.2.1 Stakeholders

An *actor* or a *stakeholder* is a person or a role which is somehow involved in a use case. In this section, we give an overview of all actors that are involved in our use cases.

We distinguish between two kinds of actors: *customer* and *employee*. Customers represent the end users of the products/services that are provided by the case study partners (SAG, IW, and EVRY), while employees represent actors that are employed by the case study partners. From the perspective of the RASEN project, the employees are the intended users of the RASEN R&D results.

The two defined categories for the customers and respectively the employees are shown in Table 2 and Table 3.

Short Name	Name	Industry Domain	Description
C1	Customer	Business, Financial	Company external personnel working with the product to fulfill daily business or using the services on a daily business
C2	Patients	Medical	Main beneficiary of IT systems (e.g., health records)
C3	Staff	Medical, Financial	Customers working with the IT systems and software

Table 2 – Use Case Stakeholders – Customers

Short Name	Name	Industry Domain	Description
E1	Business Analyst	Business	In charge of refinement and definition of requirements and specifications
E2	Software Developer	Business, Medical, Financial	Implementation of the requirements and specifications in software
E3	Source Code Analyst	Business	Conducts the analysis of source code using tools and software
E4	Binary Code Analyst	Business	Conducts the analysis of intermediate binary code fragments
E5	Penetration tester	Business	Conducts penetration tests
E6	Suite integration tester	Business	Integrates and tests the components
E8	IT staff	Medical	Administration, configuration and maintenance of IT systems
E9	Management/financial staff	Medical	Monitoring, control, and steering of finances and companies
E10	Tester/Security Tester	Medical, Financial	Builds and executes comprehensive testing plans and security tests
E11	Bank employees	Financial	Direct point of contact to bank customers
E12	IT Support	Financial	Hotline and support for customers

Table 3 – Use Case Stakeholders – Employees

3 Case Study: Software AG

Software AG was founded in 1969 in Darmstadt Germany and is among the top 10 fastest-growing technology companies in the world. It is ranked a “Leader” in eight analyst categories, including Service-Oriented Architecture (SOA), Business Process Management (BPM) and integration just to name a few.

In the sequel of this section the case study from Software AG is described which covers the Software Development and Security Testing process in the field of enterprise business software.

3.1 Industry Sector: Enterprise Business Software

Software AG has a vast solution portfolio which helps companies to optimize and modernize existing technologies to achieve business results faster. Different software solutions belong to Software AG’s key competences like Adabas, the first high-performance transactional database, ARIS -- the first business process analysis platform, the first B2B server, SOA-based integration platform, webMethods; and pioneering big data technology with Terracotta’s BigMemory.

By a rich software portfolio and a consulting branch (IDS Scheer Consulting) Software AG offers a variety of end-to-end solutions that deliver low total cost of ownership and high ease of use. Software AG's industry-leading brands, ARIS, webMethods, Adabas, Natural, CentraSite, Terracotta and IDS Scheer Consulting, represent a unique portfolio encompassing: process strategy, design, integration and control; SOA-based integration and data management; efficient management of big data; process-driven SAP implementation; and strategic process consulting and services.

The products produced and sold by Software AG are typically used by customers or consulting companies to build business critical applications that run at customer’s sites. As an example, Software AG’s business process execution product is used by many customers to automate core business processes.

3.1.1 Software Portfolio

Software AG’s portfolio encompasses different solution suites addressing enterprise needs. An overview of Software AG’s solution suite is depicted in Figure 2, which encompasses the areas of *Enterprise Architecture*, *Process Intelligence*, *Process and Composite Applications*, *Enterprise Service Bus*, and *Software for Service Oriented Architecture* (SOA) *Governance*.

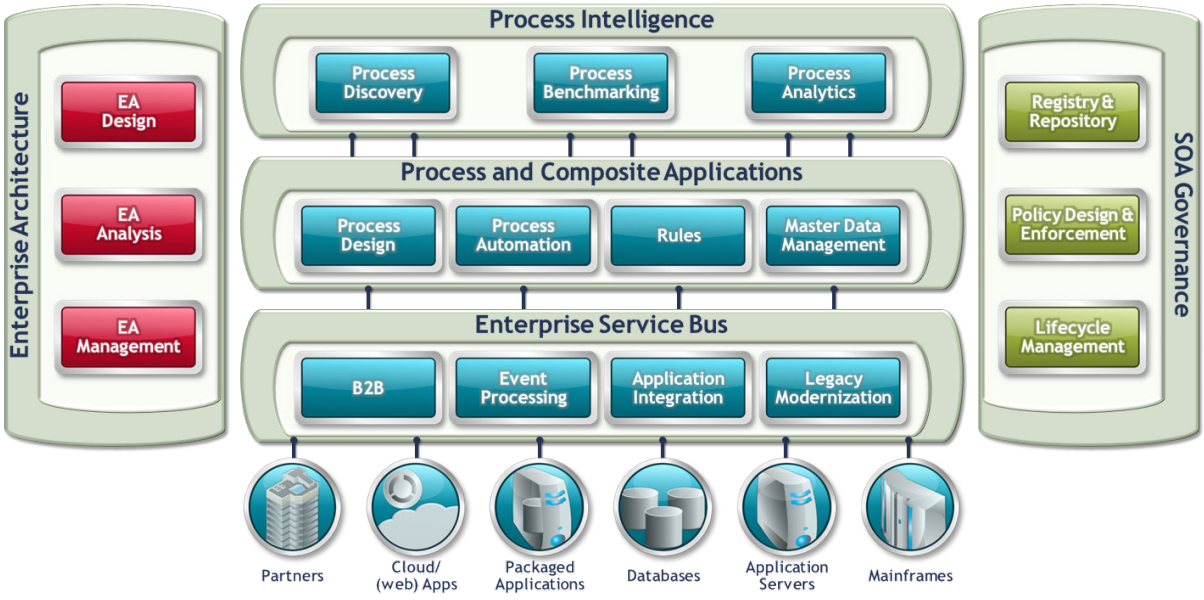

Figure 2 – Software AG Product Portfolio

The software is manifold and the mostly widely used software products are as follows:

3.1.1.1 TERRACOTTA

Terracotta is a platform for big data management in large Java-based environments. The technology enables huge volumes of data for transaction-oriented systems to be stored in-memory (big memory), improving system performance many times over. Application scenarios include real-time data processing in payment transactions, fraud detection and high-volume data availability for making travel reservations.

3.1.1.2 ARIS

ARIS is business process analysis (BPA) and optimization platform. In addition, ARIS is also used by many companies and government agencies for enterprise architecture management (EA) as well as governance, risk and compliance management (GRC). In the recent version ARIS offers support for innovative collaboration and cloud functionality.

3.1.1.3 WEBMETHODS

The integration and automation of applications as well as business process management are the primary focuses of webMethods. In addition to messaging, integration server, enterprise service bus and the SOA registry, the platform also contains functions for complex event processing and a comprehensive mobile suite. Adapters for numerous platforms and ERP systems as well as for B2B and a trading network complete the offering.

3.1.1.4 ADABAS

Adabas is currently used by thousands of business and public administration customers for data management and application development in their core business. The database is known to bring certain advantages with respect to Index-Processing, large datasets or access rights which can be defined down to field-level. The latest version of ADABAS allows almost unlimited data storage capacities and real-time data access from every location. In addition to the standard ADABAS database which stores data in a packet format (this format allows periodic groups or multiple fields) a relational database type exists.

3.1.1.5 NATURAL

Natural is a software development environment from Software AG for the development of applications which was formerly used on main frame machines. By today it is supported by many mainframe, UNIX, Linux, and Windows operation systems and supports a 4GL-programming (4^{th} generation language) language named NPL (Natural Programming Language) often cited as NATURAL.

Natural can access a variety of different DBMS (database management systems) using highly efficient proprietary database access commands as well as standard SQL commands. Access on supported databases is realized using native i.e. DBMS specific database drivers. Natural Source Code is compiled into an intermediate code which is in turn interpreted by the Natural run-time environment, similar to a java Virtual Machine.

3.1.2 Technical Aspects and Customer Requirements

Software AG delivers its products to customers worldwide. Their businesses rely on this very complex suite of interrelating products for their business-critical and highly sophisticated applications. Typically, such applications are distributed, logically and geographically, and encompass hundreds of installations, servers, and processing nodes. As customers rely on this software, products should not expose vulnerabilities, but reflect the state of the art technology and obey security or technical risks. Failing to meet customer expectations would result in a loss of customer trust, customer exodus, financial losses, and in many cases in legal consequences and law suits. On the other hand, the impossibility to test and account for every potential security problem in advance is well-known within the field of security. Hence, the most critical and important security test cases must be identified.

Any security problem in this software could lead to a considerable damage for the customer, be it its loss of business (e.g. when a successful DoS attack prevents business processes form being pursued), loss of data (due to unauthorized access) or malicious manipulation of business process sequences or activities.

Due to these consequences, the production process of enterprise software includes various stages of testing (e.g. testing components, testing products, testing combination of products) that happen at various steps in the production process. This includes not just functional testing, but also security testing. To a large degree, testing is automated, but there are also manual test cases in the production chain. These are typically performed by dedicated testers, not by developers. Generally, the production process is organized along the lines of lean production. A continuous delivery pattern is pursued which means that in regular intervals (typically daily), a complete compile and build process for each component/product is performed. The results undergo a dedicated suite of tests, if these tests are passed successfully the component/product is promoted to a first integration stage, where it is combined with other components/products. The combination again undergoes a dedicated suite of tests (integration tests). The latter step may be applied several times, combining more products.

3.1.2.1 Key Software Requirements

Essentially, in order to retain customer expectations and demands, the following requirements must be assured in development. Key aspects of Software AG's development are described in the following as an eStandard:

- **Integration/compatibility:** Integration of software is a key aspect in the area of business suites. Essentially compatibility is a generalized definition on information technology systems which describes the ability of diverse systems to cooperate, meaning that information is exchanged. By obeying this standard adapters become feasible. Adapters in turn implement the feature of converting attributes of one device or system to those of an otherwise incompatible device or system. Adapters are essential in the world of enterprise business software which interconnects existing infrastructure components with new software systems.
- **Security** encompasses measures to prevent exceptions in the security policy of an application of the underlying system. This could be assured by authenticating and authorizing access and allowing applications only to control the use of resources which is granted to them.
- **Correctness** states that implemented algorithms are correct with respect to their specification. It essentially is sufficient to obey functional correctness which refers to the input-output behavior of the algorithm, meaning that for each input the correct output is obtained.

3.1.3 Reference standards of importance

Relevant standards which are often requested by customers are not limited but essentially address the following references:

3.1.3.1 Common Criteria for Information Technology Security Evaluation (ISO 15408)

The Common Criteria for Information Technology Security Evaluation [6] is a multipart standard which defines a common criteria framework used to specify functional security and assurance requirements of IT products and computer systems, used by vendors. The common criteria permit comparability between the results of independent security evaluations by providing a common set of requirements of the security functions of IT products and systems and for assurance measures applied to them during a security evaluation. On the basis of this, process specifications, implementations and evaluation of computer security products can be conducted in a rigorous and standard manner. Key Concepts of this standard are:

1. **Target of Evaluation (TOE):** specify the product or system that is subject of the evaluation
2. **Protection Profile (PP):** a document typically used to identify security requirements for a class of security devices in the context of a particular purpose. PPs deliver a template for

vendors and customers – looking for particular types of products which are certified against PPs of their needs.

3. **Security Target (ST):** security properties of the target are identified in this document. Security Targets usually refer to one or more protection profiles and are usually published in a way that potential customers may determine the specific security features that have been certified by the evaluation.
4. **Security Functional Requirements (SFRs):** specify individual security functions as a standard catalogue for example of how user acting in a particular role might be authenticated.
5. **Security Assurance Requirements (SARs):** describe measures taken during development and evaluation of the product to assure compliance with the claimed security functionality.
6. **Evaluation Assurance Level (EAL):** give a numerical rating between 1 and 7 (for EAL 1 being the most basic and cheapest to implement and EAL 7 being the most stringent and hence most expensive), which describes the depth and rigor of an evaluation.

3.1.3.2 NIST Publications: US Government requirements

Operations in the United States are heavily influenced by the U.S. government specifications and recommendations. The following sample illustrates some of the security relevant guidelines published by National Institute of Standards and Technology (NIST) required to successfully operate business in the U.S. market:

- **FIPS PUB 200 "Minimum Security Requirements for Federal Information and Information Systems"** [14] specifies minimum security requirements for federal information and information systems in seventeen security-related areas. Federal agencies must meet the minimum security requirements as defined herein through the use of the security controls in accordance with NIST Special Publication 800-53, Recommended Security Controls for Federal Information Systems, as amended.
- **NIST Special Publication 800-53 "Security and Privacy Controls for Federal Information Systems and Organizations"** [7] provides guidelines for selecting and specifying security controls for organizations and information systems supporting the executive agencies of the federal government to meet the requirements of FIPS 200, Minimum Security Requirements for Federal Information and Information Systems. The guidelines apply to all components of an information system that process, store, or transmit federal information.
- **FIPS PUB 140-2 "Security Requirements for Cryptographic Modules"** [9] provides a standard that will be used by Federal organizations when these organizations specify that cryptographic-based security systems are to be used to provide protection for sensitive or valuable data. Protection of a cryptographic module within a security system is necessary to maintain the confidentiality and integrity of the information protected by the module. This standard specifies the security requirements that will be satisfied by a cryptographic module. The standard provides four increasing, qualitative levels of security intended to cover a wide range of potential applications and environments. The security requirements cover areas related to the secure design and implementation of a cryptographic module. These areas include cryptographic module specification; cryptographic module ports and interfaces; roles, services, and authentication; finite state model; physical security; operational environment; cryptographic key management; electromagnetic interference/electromagnetic compatibility (EMI/EMC); self-tests; design assurance; and mitigation of other attacks.
- **FIPS PUB 180-4 "Secure Hash Standard (SHS)"** [13] specifies hash algorithms that can be used to generate digests of messages. The digests are used to detect whether messages have been changed since the digests were generated. Secure hash algorithms are typically used with other cryptographic algorithms, such as digital signature algorithms and keyed-hash message authentication codes, or in the generation of random numbers (bits).

- **NIST Special Publication 800-132 "Recommendation for Password-Based Key Derivation"** [8] specifies a family of password-based key derivation functions (PBKDFs) for deriving cryptographic keys from passwords or passphrases. The randomness of cryptographic keys is essential for the security of cryptographic applications. In some applications, such as the protection of electronically stored data, passwords may be the only input required from the users who are eligible to access the data. Due to the low entropy and possibly poor randomness of those passwords, they are not suitable to be used directly as cryptographic keys.
- **NIST Special Publication 800-131A "Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths"** [10] is intended to provide more detail about the transitions associated with the use of cryptography by Federal government agencies for the protection of sensitive, but unclassified information. The Recommendation addresses the use of algorithms and key lengths; the validation of cryptographic modules that utilize them is provided in [10]
- **NIST Special Publication 800-90A "Recommendation for Random Number Generation Using Deterministic Random Bit Generators"** [11] specifies techniques for the generation of random bits that may then be used directly or converted to random numbers when random values are required by applications using cryptography.
- **NIST Special Publication 800-92 "Guide to Computer Security Log Management"** [12] provides recommendations in facilitating more efficient and effective log management for Federal departments and agencies. Log management is essential to ensuring that computer security records are stored in sufficient detail for an appropriate period of time. Routine log analysis is beneficial for identifying security incidents, policy violations, fraudulent activity, and operational problems. Logs are also useful when performing auditing and forensic analysis, supporting internal investigations, establishing baselines, and identifying operational trends and long-term problems. Organizations also may store and analyze certain logs to comply with Federal legislation and regulations, including the Federal Information Security Management Act of 2002 (FISMA), the Health Insurance Portability and Accountability Act of 1996 (HIPAA), the Sarbanes-Oxley Act of 2002 (SOX), the Gramm-Leach-Bliley Act (GLBA), and the Payment Card Industry Data Security Standard (PCI DSS).

3.2 Relevance to RASEN

For Software AG the development of dependable and secure software is the most important aspect on which customers can rely. Hence it is essential to have an established software development process to provide software which has proven to fulfill the high expectations from customers.

This section delivers a discussion on the security aspects of Software AG's software production and highlights state of the art methodologies when developing secure software systems and enterprise solutions. By contributing knowledge and best practice to the RASEN project Software AG intends to close the gap between risk based testing, high level risk analysis of the product and security risk assessment.

3.2.1 Actors

Due to its manifold structure and instantiation at different customers sites customers are from different industry domains. The case study provided is instead more focusing on key aspects that RASEN is pursuing and hence targets the software development domain and highlights related security aspects.

- **Customers:** all technical and IT-personnel which is working on the customer's site with the configuration, maintenance or using the products for their daily business. This is for example with respect to the ARIS framework the risk manager in charge of risk assessment.
- **Business Analyst:** these people refine feature requests and consider customers' needs for up-coming software releases. Their duty is to document the requirements in accordance with the product management to define technical documents which are understood by software developers.

- **Software Development:** these people implement the technical requirements as documented by the business analyst into software. The functional requirements are derived using the specification sheet.
- **Source Code Analysis:** in charge for source code analysis which discovers security flaws using automated tools. They scales well on big software implementations and are very successful with respect to discovering buffer overflows, SQL injection flaws etc.
- **Binary Code Analysis:** instead of running on source code the binary code analysis scans the compiled byte-code, so enterprises can test comprehensively and more accurately and highlight flaws which remain uncovered by the previously applied security scans.
- **Penetration Testing:** this team is responsible for ensuring the system and software security by simulating attacks and malicious threats, which simulate authorized and not authorized users to the system. In terms of potential attacks the level of security and system vulnerability is tracked.
- **Suite Integration Testing:** this role assures the proper operation and integration of the newly developed components with other existing systems and software parts. After a successful integration testing, the component is prepared in the following step for final integration into a software product or software bundle. This software package is then promoted to other systems for sale or integration into existing software suites.

3.2.2 Targeted Software Systems

The case study which Software AG's brings to the RASEN project describes the software development process which is considered as the major focus of a software vendor. It is considered as the main area of expertise with the highest relevance to RASEN and the most critical for successful business.

The software security is not only related to a specific product but encompasses the security of the whole software. This makes it very challenging to face this case study with state of the art methodology and in particular results which Software AG expects from the project. Currently this task is achieved using a combination of source code scanning, scanning of binary code, and penetration testing intermediate testing phases, very complex and hence not transparent.

The current production process of Software AG's software developing cycle is the most suitable target of the RASEN project. Risk assessment is considered in the current production process of the software development cycle, but it is performed on shipping-ready or shipped products or suites. As a consequence, a new process has to be established that shifts the identified risk assessment to an earlier stage in the production process, in order to be able to combine this with security testing. Furthermore, the testing infrastructure in place has its structures and rules.

3.3 Use Case Descriptions

This section gives a detailed overview about of Software AG's use case proposed for the RASEN project. It turns out that the software production process is the most critical process which is detailed in the following.

3.3.1 Description of Current Processes

In the current process there are two points where we can manage things well. One is the level of the source code. We can analyze the existing code and the new code that is being added. We can define what the risks are in the source code and how to look for them. But we cannot aggregate it up into an overview. On the other hand, we can analyze the risk at the highest level of every product and estimate various parameters there. Unfortunately, it is also impossible to break it all down into smaller components to reach the lower levels.

So we are left with two disjoint models. One model describes at the very abstract level the risk analysis of the product while the other lets us estimate the security through the code quality and correspondence to certain security rules. There is a gap in between that does not allow us to place any correspondence of one to the other. This gap causes a loss of transparency, introduces a security risk all by itself and makes risk based testing impossible.

What we are looking for is tools that would allow us to bridge the gap between the high level risk assessment and the low level code analysis and testing, create a correspondence and input the results of the low level assessments into the risk analysis. Composition of the analysis results into the higher levels would allow us to verify the results of the risk analysis at the higher level and decomposition would then feed the results of the residual risk analysis into lower levels to influence the testing and analysis at the low level.

3.3.1.1 Use-Case Scenario I: Enterprise Software Production Process

Name (ID)	Enterprise Software Production Process (SAG_S_1)
Category	Security Issue
Brief Description	This process consists of different elementary steps. Starting from the Analysis of the customer's expectation, software is developed and tested and finally bundled into a product.
Purpose/ Requirement	The purpose of this step is to start from the customer's need to develop security tested software. As a prerequisite the requirement engineering has to assure that the requirements are captured in a feasible and understandable way understood by the core development team. As additional requirements the testers must be familiar with underlying regulations and expectations and the deployment can occur in a properly set-up infrastructure.
Primary Stakeholder	Business Analyst Software Developer (Team) Source Code Analyst (Team) Binary Code Analyst (Team) Penetration Tester (Team) Integration Tester (Team)
Narrative description	The software product development occurs in different steps: 1. Feature definition (Business Analyst) 2. Refinement I accordance to current development (Business Analyst + Chef Software Engineer + Product Manager 3. Development of the Specification (Software Development Team) 4. Source scanning (Security Team) 5. Unit testing (Testing Team) 6. Binary scanning (security Team 7. Integration testing 8. Penetration testing 9. Suite integration testing

Table 4 – Enterprise Software Production Process

The following section relates the above mentioned scenario to the RASEN project and highlights in particular relevant processes and use-cases for future analysis within the project.

3.3.2 Key Figures in the Security Testing Process

Currently, 22 products are involved in the security testing process with increasing tendency. Essentially all of these tools contribute differently to the eventually received security. To decide whether a security run is successful and the total security contained in a product increased, a metric is defined.

Different figures contribute to this metric which are collected from different phases of the security testing process. In the following some of the figures are described with their corresponding phase of the development process.

1. **Source Code Scanner**
    a. **FindBugs Bug Density:** describes the number of potential bugs found in the code by the *FindBugs*[2] source code scanner. This number becomes higher when the code quality goes down. An increase may indicate a higher risk through a higher likelihood of problems in the code in general and in security in particular.
    b. **PMD Bug Density**: accordingly to the figure from before, this number describes the same as FindBugs, but only indicates the density of general quality issues found by the *PMD*[3] source code scanner. As denoted above a higher number may indicate a higher potential risk.
2. **Binary Code Scanning**
    a. **Veracode score**[4]: is a composite number that depends on the number and severity of potential security problems found in the code. It may be between zero and 100, the higher number reflecting lower number of severe vulnerabilities. Lower numbers thus reflect a higher risk of exploitable vulnerabilities.
3. **Composite Figures:**
    a. **Coverage:** is expressed in percent and shows how much of the code is covered by the scanners. Generally speaking, an unscanned portion of the code is a dark box that we know little about. The higher the percentage for the code coverage - the better, the lower the risk of discovering problems that may have been found by scanners if the code was scanned.
    b. **Security defects number**: a number of security defects outstanding in the bug tracking system against a product. The higher number of security defects indicate a higher risk of exploitable vulnerabilities in the code. This number is more "real" than others because it reflects the confirmed security vulnerabilities as opposed to potential security vulnerabilities reported above. Therefore, normally this number is given a higher weight in the risk analysis.

In addition to afore mentioned figures, deltas are computed for each of the respective figures which compare the previous to the recent values and thus make the evolution of figures visible and comparable.

3.3.3 Security Testing involved in Software Production Process

Software AG is for a large part a software development company. The software development processes used are fairly formalized by necessity reflecting the large number of software developers spread across multiple sites around the world. The process of development is driven by the customer requirements filtered and prioritized by the product managers then fed into the product development teams. The development teams take care of developing the features and tests in parallel, making sure that the software is unit tested on every single day.

Key phases of the software production process are displayed with their order of processing in Figure 3 below. In a first step customer demands in terms of a feature catalog are specified into system requirements. These functional and non-functional requirements are refined in a second process step to align them with the product definitions and development plans. In turn the development implements the refined requirements and components.

The produced source code is constantly scanned for deficiencies in the *source scanning* phase. Typically these tools are designed to run over the source code several times during development, each time fixing or investigating a major problem. Operating on hundred thousands of lines of input under one second, software source scanners are quite fast and help to highlight common coding errors or problematic code areas which lead to faulty code or even introduce security issues within the code.

[2] http://findbugs.sourceforge.net/
[3] http://pmd.sourceforge.net/
[4] http://www.veracode.com/

After successfully passing this stage “Unit Testing” assures the functional correctness of the implemented software. Subsequently *binary scans* are conducted daily on the compiled sources which highlight binary specific defects. Static binary code scanners are used to detect vulnerabilities through disassembly and pattern recognition. As a clear advantage of this approach that the use of binary code scanners provides over source code scanners is the ability to look into the compiled results and factor in vulnerabilities which were created by the compiler itself. Furthermore, also code from libraries or other software fragments only available as software library functions can be examined.

In the following phase integration testing is done where individual software modules are combined and tested as a group. Essentially this testing step takes as its input modules that have been unit tested, groups them into larger aggregates, and delivers as its output an integrated system.

In the *penetration test* the software security is evaluated by simulating an attack from malicious outsiders. This may either happen in terms of a malicious outsider (who does not have an authorized access to the organization’s systems) or a malicious insider (who has some level of authorized access). The penetration test essentially highlights the following problems if they:

1. identifying higher-risk vulnerabilities that result from a combination of lower-risk vulnerabilities
2. identifying vulnerabilities that may be difficult or impossible to detect with automated network or application vulnerability scanning software
3. assessing the magnitude of potential business and operational impacts of successful attacks
4. testing the ability of network defenders to successfully detect and respond to the attacks
5. providing evidence to support increased investments in security personnel and technology

After successfully passing this final test, the software module is integrated into the software suite and tested for compatibility and within a final suite or product.

After the software is written and submitted to the version control system it passes the build infrastructure that re-creates the complete software suite every day and takes care of unit testing the components. The software then passes several rounds of regression and integration testing to emerge into a fully tested software suite that may be delivered to the customer. During the testing phase the software is analyzed with several tools from the security point of view, including source code analysis, binary scanning and penetration testing.

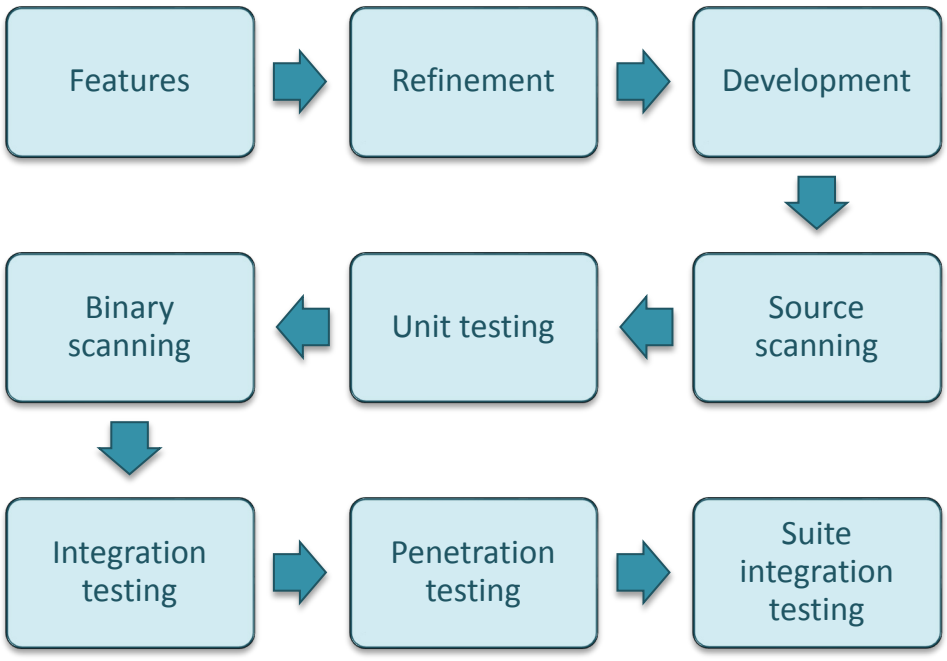

Figure 3 – Software Development and QA Process

3.3.4 Expectations from RASEN

The results that Software AG expects from the RASEN project will address ways to improve the software production process and relate security testing with risk assessment methodology. Thus the scenarios described below are very suitable within the RASEN context since they address the ideas following research which will take place in the project. What all of these have in common is to reduce prohibitively expensive tests using conventional methods to an acceptable level by combating:

- the huge size of tests
- the complexity of security tests
- increasing the level of automation
- pinpointing attention to potentially problematic areas (instead of “carpet bombing”)

In the following desirable areas are described which identify the above issues and combine them with the strength of the RASEN approach.

3.3.4.1 Risk Analysis of newly implemented Features

Whenever new features are implemented, the requirements analysis contains a careful assessment of needs or conditions that need to be met by the new or altered product. This takes into account existing possible conflicts with other requirements of various stakeholders. In this sense when analyzing, documenting and validating system requirements the level of risk can also be estimated. Hence the development of new features should be accompanied with a risk analysis and possibly be even extended during the software production process as unforeseen issues and open questions come up.

In this sense risk analysis is continuously assuring an exhaustive list of addressed risks which eventually leads from the list on the level of new features up into the final component and eventually contributes to the risk level on suite level. Hereby the overall risks can be estimated of how the risk level of the overall suite is affected by the implementation of this single feature. Alternatively software products which encompass a set of components expose a combination risk which they inherit from their core features. In this sense not only the question about the risk of singular features is addressed, but also issues of how the composition of these features affects this feature.

As an open issue we expect such a risk analysis feature to be developed within the RASEN project which addresses this problem.

3.3.4.2 Risk selection and mitigation

This scenario aims for risk selection and mitigation. Suppose a new feature is implemented and eventually integrated into the final product of a product suite. According to the scenario A from before the resulting risk of the final software encompasses all risks from its parts.

Each product is implemented according to requirements which aim the deployment in an intended environment. In fact the risk awareness in different environments could vary in a sense that the product may be suitable for an environment for which it was initially designed but it exhibits an unacceptable risk which prohibits the use in another more critical environment due to an unacceptable risk.

To mitigate the overall risk to a justifiable level, risky features must be identified which contribute excessively to the overall resulting risk. Once these features are identified the risky program code could be altered to mitigate the risk or the feature could simply be dropped or replaced. In addition a measurement to categorize risks is highly advantageous to derive the level of risk exactly and correlate it to the affected features. As an example this could mean at the very end that either a feature is altered or two other features replace it in the software in order to obtain the targeted level of overall risk. Or addressing this example from a different perspective: which features have to receive the mitigation attention to obtain the desired level of residual risk.

3.3.4.3 Compositional Risk Tracking

In this scenario a new feature is implemented and integrated into different components. In the very beginning, the feature is analyzed and its risk is assessed. After the security testing no issues are discovered and finally the new feature is integrated into components A and B which are deployed in different instances.

After some time a previously unknown vulnerability is found in the specific feature which is deployed in the component and tracked which other components are also affected by this issue. In this sense the vulnerability found in the code is tracked to features which contain the code and tracked even further to other components which also depend on this code fragment.

Within this context it is essential that the tracking works in both directions, the security impact of the feature is analyzed based on the risk analysis and the risk analysis of the feature is automatically reflected in the risk analysis of the product.

3.3.4.4 Product Prioritization and Risk Rating

At Software AG the list of software products is extensive and the implementation of additional security tools, processes and measures across several hundred developers is understandably a challenge. Even more so as the development of software products, adapters, and components is distributed across several R&D centers around the globe.

Nowadays the results of comparative product risk analysis are used to prioritize the mitigation of different defects and risks. In this sense products that are currently deemed to have an elevated risk rating receive the newest tools, updates and security reviews first with others following suit.

In the context of the RASEN project the risk analysis is supported by the risk assessment and risk rating of the tool chain, in a sense, the tools are expected to compute the proper level of acceptance according to other risks and prioritize the development of products accordingly.

4 Case Study: Info World

Info World (IW) is a supplier of IT solutions dedicated exclusively to the healthcare field. The company provides customized modular integrated solutions for both clinical and economic management of healthcare facilities. Info World also offers training, service and maintenance for products in its portfolio and is currently active in Europe, America, Africa and Asia.

Info World products are implemented in a modular fashion so they can be combined into customized configurations. In addition, Info World provides deployment, training and support services to assist customers in using the delivered products in order to ensure optimal patient care.

4.1 Industry Sector: Medical Informatics Domain

The present section details Info World's domain of activity highlighting general technical and legal issues and briefly details the actors that represent the company solutions' end users.

4.1.1 Technical and Legal Aspects

Info World is a Hospital Information System (HIS) supplier for more than 70 healthcare units including the National Health Care Public System (that includes hospitals, blood banks, clinics, institutes, health insurance houses and others), Romanian Private Healthcare (various private Medical Centers, Policlinics and Laboratories), GP's consulting centers, pharmacies and more. As such, Info World products must adhere by stringent technical, operational, legal and security requirements that must be taken into account during the analysis, development, implementation and maintenance of its solutions.

From a technical standpoint, all implemented solutions must adhere to stringent requirements of security in order to protect patient well-being, confidentiality of sensitive information and to prevent unauthorized access to the protected systems, both from the outside and within the local network where such solutions are deployed.

Info World acknowledges the importance of using well established standards and methodologies in the development, testing and maintenance of its product portfolio. As such, all IW products are designed to adhere to HL7 guidelines. HL7 (Health Level 7)[5] is an international non-profit organization involved in the development of several interoperability standards for medical informatics such as HL7 v2.x and HL7 v3.0. Currently all Info World products are planned and implemented according to the HL7 v3.0 standards.

The implementation of this internationally recognized family of standards regarding exchange, integration, and retrieval of electronic health information across the IW product stack facilitates the design and implementation of robust and secure products that are able to easily exchange messages between them and with external implementations, ultimately allowing for the interconnection of several such systems designed by different vendors in different areas of the globe.

As HL7 branches exist in over 40 countries across the globe, the standards the organization promotes are seeing ever widening acceptance and implementation across eHealth products from all over the world.

As an important player in the field of Romanian healthcare solutions, Info World has spearheaded the creation of the HL7 Romania Organization[6] in order to promote the informatization of the Romanian medical sector and to provide readily accessible information regarding HL7 standards.

Aside from technical issues, healthcare oriented software also has to abide existing legal regulations, both at EU and member state levels. As Info World is active in many areas of the globe (Europe, the US, Africa) it is imperative that these aspects are taken into account from the early stages of solution analysis and design. Also, the additional burden represented by testing and proving compliance of the provided solutions with the existing legal framework at both international and national levels must be mentioned.

[5] Level 7 Home - http://www.hl7.org/index.cfm
[6] Health Level 7 Romania - http://www.hl7romania.ro/

As the main market for Info World solutions is currently Romania, the relevant parts of the company's involvement within the RASEN project will target compliance with existing norms within the EU and specific laws and regulations coming from Romanian lawmakers.

The most important piece of legislation at European Union level that impacts Info World's solutions is the *Data Protection Directive*, officially the 95/46/EC [1] Directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data. The Directive is a direct consequence of Article 8 from the ECHR (European Convention on Human Rights, of which all EU countries are signatories), which provides the right for one's "*private and family life, his home and his correspondence,*" to be respected within certain restrictions.

The 95/46/EC Directive defines *personal data* as "*any information relating to an identified or identifiable natural person ("data subject"); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity*" (art. 2 a). The term *processing* is defined as "*any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction*" (art. 2 b)

In principal, processing of personal data should only happen when three categories of conditions are met:

- Transparency
- Legitimate purpose
- Proportionality

The Directive states that the responsibility for compliance with 95/46/EC rests on the shoulders of the natural or artificial person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data; (art. 2 d).

More so, the 95/46/EC Directive states that its regulations are in place not only for data processors that are situated inside the EU, but also for processors located outside the EU but which use equipment hosted within the bounds of the EU.

As European Directives are not legally binding for citizens, each EU member state was required to set up its own legislation in order to implement the requirements of the 95/46/EC. More so, each member state must set up an independent body having the task of monitoring the data protection level within the given member state and starting legal action when violations of the data protection regulations has been detected.

Each controller that processes personal data must first notify the supervisory board and provide at least the following information that is kept in a public register:

- Name and address of the controller and of his representative, if any.
- The purpose or purposes of the processing.
- Description of the category or categories of data subject and of the data or categories of data relating to them.
- The recipients or categories of recipient to whom the data might be disclosed.
- Proposed transfers of data to third countries.
- General description of the measures taken to ensure security of processing.

The Romanian authority with competence in monitoring the processing of personal data is the National Authority for the Oversight of Processing of Personal Data (in Romanian "*Autoritatea Națională de Supraveghere a Prelucrării Datelor cu Caracter Personal*"[7]) that was enacted using Law 102/2005.

[7] National Authority for the Oversight of Processing of Personal Data - http://www.dataprotection.ro/

The acquis of the 95/46/EC Directive was implemented in Romania by the 677/2001 Law that guarantees the independence of the regulatory body from all public or private companies and associations.

As the directive was established before the wide availability of the Internet, there is very little jurisprudence regarding the online processing of personal data of EU citizens by entities outside the EU. Such online businesses will still process some data on the EU citizen's equipment as the user accesses the provided services using client computers that are located within the EU.

A new EU directive, called the European Union Data Protection Regulation [2] (draft available since January 2012) will extend existing legislation to cover all entities that process data of EU citizens regardless of their location.

By taking technical, security and legal aspects into account Info World believes the medical informatics domain to be an important and self-standing domain of competence that is in constant evolution due to a plethora of factors. First, the technical side of the field can be mentioned. As software systems become more complex and interconnected they become increasingly difficult to develop given the increasing expectations customers and patients have from such solutions.

A particular area of concern on the technical side is raised by the issues of privacy and confidentiality of information: by its very nature medical software handles highly sensitive patient information the loss or unauthorized access to which can bring about loss of life together with severe legal repercussions against both Info World and its partners in the medical field.

Concerning legal aspects, Info World and its clients must have the right to process sensitive personal information such as medical history and records and therefore must possess all required certifications according to Romanian and International law. As discussed above, legislation is not a static field in itself, with new regulations developed to cover or refine aspects that were left untreated in previous regulations. In this regard the newest efforts of the EU regarding the protection of personal information (the European Union Data Protection Regulation), currently in a draft phase must be mentioned. When they become mandatory both Info World and its partners must ensure immediate and transparent compliance in order to enable the continued operation of the implemented electronic medical infrastructure.

4.1.2 Actors

Info World solutions are widely used within the country and abroad in diverse clinical and paraclinical settings such as hospitals, private clinics, blood banks, health insurance houses and so on. As the provided solutions cover all aspects of clinical management including financial and management issues, the end users also come from different specialty backgrounds, such as:

- **Medical staff**: physicians, nurses, pharmacists, etc., having associated roles, allowing access to different sections of the application: encounters, laboratory, pharmacy, etc. Medical staff uses the system for personal data collection when the patient is recorded for the first time, diagnoses identified during the patient's encounters, clinical and paraclinical analysis data, drug prescriptions etc. The roles ensure the proper access to the applications areas, accordingly with the responsibilities assigned to each role, preventing overlaps, assuring data consistency and enabling auditing activities.
- **IT staff**: system engineers, network and database administrators who maintain the system, applications and infrastructure and having administrative role. IT staff is involved in operations like database backups/restorations, creation and maintenance of servers' security policies, antivirus/antimalware actualization, firewall policies, communication infrastructure maintenance, disaster recovery and so on.
- **Management/financial staff**: people from different departments using reports facilities in order to control and monitor the hospital's activities. Their role doesn't imply data modifications, but only queries of data, running reports like financial balances, accounts turnover, profit and loss situations, etc.

- **Patients**: role to be used in portals, allowing the visualization of personal medical data, reports regarding the modifications upon personal data as the patient is the main beneficiary of his own health record.

4.2 Relevance to RASEN

This section contains a brief discussion regarding issues that pertain to the RASEN implementation as important contributions to the state of the art on both technical and legal aspects related to Info World's activity in the eHealth field are possible. As discussed in Section 4.1, eHealth products face particular technical, security and privacy issues that must be dealt with by any organization providing such products and services.

Info World's participation in the RASEN project is the latest bid to build upon its knowledge in the field of developing secure software systems and take part in international efforts aimed at further improving the state of the art. By contributing its specific expertise to the RASEN project Info World can contribute to the evaluation and use of new tools and methodologies for the analysis, design, development and testing of complex networked medical software.

4.2.1 Actors

This section briefly details the participating actors in Info World's case study for the RASEN project. They include people from the development and testing teams that will directly benefit from the software artifacts resulting from the RASEN implementation:

- **Developers**: role fulfilled by highly trained Info World specialists that are responsible for the analysis, design and implementation of the company's product stack. Their working processes are expected to be improved significantly by the implementation of the RASEN project's output in their workflows, thus helping them in developing and providing comprehensive secure solution faster.
- **Testers**: role fulfilled by specialists that build and execute comprehensive testing plans to ensure reliable, correct and secure operation of Info World's solutions. The expected outputs of the RASEN project are expected to provide significant improvements to their workflows. Info World expects RASEN to enable a formal integration of risk assessment activities within software development and testing processes together with a better targeted plan for building, prioritizing and assessing test set results.

Users fulfilling the *developer* and *tester* roles stand in the frontline of beneficiaries of the RASEN project's implementation. New methodologies concerning risk assessment and its consequences regarding the testing of applications under development will provide an immediate positive impact on their work, allowing for a more thorough, formal assessment of existing risks and testing requirements; also, new knowledge gained during the implementation of RASEN is expected to be materialized into tools that will enable formal risk assessment together with a more targeted approach for performing security and vulnerability testing, thus improving confidence in the delivered solutions.

End-users in roles such as *medical staff*, *IT staff* and *financial/management staff* that were detailed in Section 4.1.2 will indirectly benefit from the existence of comprehensive tools that are more robust, secure and have a shorter time to market than was possible before.

Last but not least, the main beneficiaries are patients themselves who will benefit from the advantages provided by a more secure solution that implements the latest standards of security and confidentiality regarding the processing, storage and retrieval of their highly sensitive personal data.

4.2.2 Targeted Software Systems

Info World's case study for the RASEN project consists of several software components that provide the backbone for most of the company's product stack. Info World solutions are developed using the Service Oriented Architecture (SOA) methodology and implemented using the latest Microsoft tooling and .NET framework available.

The software systems targeted in Info World's case study for RASEN comprise several crucial web service components that provide key functionality in areas such as patient and client organization management, management of patient – organization interaction, management of medical records and documents and vocabulary services providing vocabulary coding information, mappings and translation.

All business services are secured using state of the art technologies that rely on well-known and trusted principles such as asymmetric cryptography, digital signatures, single-sign-on and more. The central hub of these technologies is the Security Service that provides required functionality to enable Authentication and Authorization across the platform.

The following paragraphs briefly detail the software systems targeted by the case study together with a description of Info World's security service detailing key aspects regarding implemented standards and methodologies.

4.2.2.1 Admission, Discharge, Transfer Service (ADT)

The role of the ADT component is to provide functionality regarding the management of patient encounters in the context of a HIS application. A patient encounter is defined as any interaction taking place between a patient and a clinical organization, either fixed or of a mobile nature (e.g. an ambulance).

Patient encounters can be of several types, such as appointments, admissions, discharges, transfers and consultations, each of which have specific data attributes that are mandatory (such as admission location, admitting physician and so on…).

Beside the management of patient encounters, a key aspect of this service regards the interoperability with different services of the same type and even with different HIS applications in order to enable storage and retrieval of patient information across such systems. The main enabler of such scenarios is the HL7 specification that provides a complex framework regarding how to achieve interoperability between different implementations. The HL7 standards provide the list of mandatory attributes that characterize patient-centric interactions together with formalization of messaging formats to facilitate secure interchange of messages between different systems that implement the HL7 specification.

The ADT service enables the management of the most important patient-centric interactions such as scheduling patient encounters, scheduling and carrying out patient admission and discharge together with the required functionalities for updating patient data.

4.2.2.2 Entity Identification Service (EIS)

The EIS component is responsible with the management of various entities across the platform. Based on the Healthcare Services Specification Project (HSSP) [3] EIS is responsible for providing CRUD[8] scenario for entities represented within the platform. Entities are stored using entity-identifying characteristics (e.g. demographic information for patients) and manipulated through an entity ID provided by EIS after creation of entities.

HSSP EIS specifications are designed for the management of medical entities (patients, doctors, medical organizations, clinics, hospitals, etc.). Info World's EIS component relies on the HSSP EIS specifications for entity management and as such is interconnectable with implementations abiding the same compatibility specifications.

Info World's EIS service provides the required functionalities for working with medical entities as follows:

1. **Entity Creation** – Creates a new entity within the system.
2. **Entity Update** – Updates the information stored for an entity.
3. **Entity Deletion** – The EIS system provides logical deletion of existing entities.
4. **Entity Read** – Existing entities can be retrieved from the service's data store using their unique **ID** or by characteristic traits.

[8] Create, Read, Update and Delete

When the platform is in its setup phase (e.g. for implementation within a new medical organization) the deployment team[9] must set up the EIS service using specific information pertaining to the install location such as active domains, organizational structure, medical personnel and so on. Such actions are available by using a MMC (Microsoft Management Console) snap-in that allows connecting to the EIS service and performing administrative tasks.

4.2.2.3 Retrieve Locate and Update Service (RLUS)

The RLUS component is a service that provides functionality for locating, retrieving and updating clinical and non-clinical information. Typically, the component is employed to provide CRUD functionality for patient-centric medical data such as analysis results, medical records and so on.

The principal use cases provided by RLUS are:

1. **Create RLUS Entry** – Allows the creation of a new entry within RLUS. The newly created entry receives a unique GUID (Globally Unique Identifier) using which it can be accessed.
2. **Update RLUS Entry** – Allows updating the contents of an existing entry within RLUS.
3. **Delete RLUS Entry** – Provides logical deletion for existing entries.

4.2.2.4 Enterprise Vocabulary Service (EVS)

The vocabulary service provides the required functionalities for covering the use, mapping and translation of clinical vocabulary systems within the implemented platform.

The vocabulary service is based on the HL7 Common Terminology Services (CTS) v1 [4] standard which was developed as an alternative to a common data structure. Instead of specifying what an external terminology must look like, HL7 has chosen to identify the common functional characteristics that an external terminology must be able to provide.

There are two distinct layers between the HL7 Version 3 message processing applications and the target vocabularies. The upper layer, the Message API (Application Programming Interface), communicates with the messaging software, and does so in terms of vocabulary domains, contexts, value sets, coded attributes and other artifacts of the HL7 message model. The lower layer, the Vocabulary API, communicates with the terminology service software, and does so in terms of code systems, concept codes, designations, relationships and other terminology specific entities.

A vital concept within the EVS specification is the *CodeSystem*. It represents the characteristics common to all code systems used within the HL7 environment. HL7 also maintains an internal registry (metadata) about code systems themselves – a code system registry. This registry is intended to function as a central repository of metadata about any code system that may appear in an HL7 message, be it internal to a site or system or commonly used and sanctioned between systems.

Registration does not constitute ‘sanctioning’ from an HL7 standpoint. It simply records a reference. The registration process also assigns a code system identifier (OID) for a code system if one doesn’t already exist.

A *CodeSystem* may define zero or more *CodedConcepts*. A coded concept represents a class or concept within a particular domain of discourse. Every *CodedConcept* must be defined in exactly one *CodeSystem*. Once defined, the meaning of a coded concept may not change. Existing coded concepts may be retired and new coded concepts may be added, but once defined, the meaning of a coded concept must remain static.

[9] The deployment team is responsible for the correct installation and functioning of Info World’s solutions within client locations.

The EVS implementation provides a plethora of functionality for entities relying on enterprise vocabularies; the main actors expected to interact with the implementation are:

- **Message Creation Software** – Software that is involved in the creation of HL7 messages. From a vocabulary perspective, this process involves the translation of internal messages and data into the syntax and semantics of the HL7 Version 3 standard.
- **Message Processing Software** – Software that receives, decodes, and acts on the content of standard HL7 Version 3 messages. This process may include validation, translation and inference steps.
- **RIM (Reference Information Model) Modelers** – A combination of tools and people that create and define HL7 Message content.
- **Software Developers** – The people who build the software that creates, validates and processes HL7 Version 3 messages.
- **Vocabulary Translators** – A combination of tools and people that translate the abstract HL7 Version 3 specification into the structure and terms of actual data processing application.

Due to Info World's efforts of providing complex, interoperable software, the EVS component lays the foundations for many other more advanced services such as ADT, EIS and RLUS which are described above.

4.2.2.5 Security Services

Info World's Security Services represent the foundation of the company's efforts in ensuring the security and confidentiality of sensitive patient data. The implemented components are based on well-established standards and practices such as:

- LDAP protocol;
- WS-Security specification;
- X.509 certificates.

These services are in charge of providing key security functionality:

- Confidentiality – encrypted message.
- Integrity – message hasn't been tampered.
- Authentication – prove identity.
- Authorization – role based access.
- Accountability – audit trail.
- Policies – mutually agreed by involved parties.

From the client application perspective, the security services are in charge of:

- Authentication:
  - SAML (Security Assertion Markup Language) assertions verified by the called service.
- Role based authorization:
  - Stored roles looked up using LDAP.
  - Policies defined using XACML (eXtensible Access Control Markup Language) language.
- Record level authorization.
- Audit trail.

The audit services provide the means to address the issues of liability management, asset protection and quality of service. To facilitate a timely response to policy violations, security incidents or

infrastructure and application failures, the project supports monitoring, logging, analyzing, and reporting on every level of its architecture.

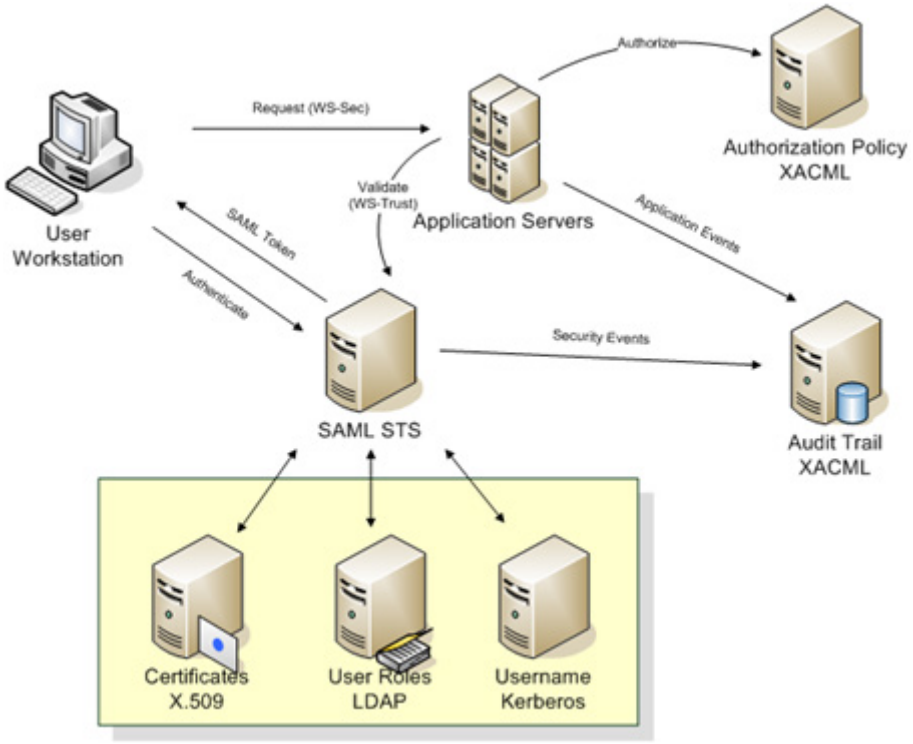

Figure 4 – Architecture of security services

All components of the Security Services use well known and tested standards in the domain, which ensures the robustness of the provided implementations and facilitates interoperability with similar services.

In the following paragraphs the security standards employed are briefly described:

4.2.2.5.1 WS-Security

The protocol[10] contains specifications on how integrity and confidentiality can be enforced on Web services messaging. The Web Services Security protocol includes details on the use of SAML and Kerberos, and certificate formats such as X.509.

WS-Security describes how to attach signatures and encryption headers to Simple Object Access Protocol (SOAP) messages. In addition, it describes how to attach security tokens, including binary security tokens such as X.509 certificates and Kerberos tickets to messages.

WS-Security incorporates security features in the header of a SOAP message working in the application layer. Thus, it ensures end-to-end security.

4.2.2.5.2 WS-Trust

WS-Trust[11] is an Organization for the Advancement of Structured Information Standards (OASIS) standard that provides extensions to WS-Security, specifically dealing with the issuing, renewing, and validating of security tokens, as well as with ways to establish, assess the presence of, and broker trust relationships between participants in a secure message exchange.

[10] https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=wss
[11] http://docs.oasis-open.org/ws-sx/ws-trust/200512/ws-trust-1.3-os.html

4.2.2.5.3 SAML

The Security Assertion Markup Language (SAML) is an XML-based standard for exchanging authentication and authorization data between security domains, that is, between an *identity provider* (a producer of assertions) and a *service provider* (a consumer of assertions). SAML is a product of the OASIS Security Services Technical Committee.

The single most important problem that SAML is trying to solve is the *Web Browser Single Sign-On* (SSO)[12] problem. Single sign-on solutions are abundant at the intranet level (using cookies, for example) but extending these solutions beyond the intranet has been problematic and has led to the proliferation of non-interoperable proprietary technologies. SAML has become the definitive standard underlying many web Single Sign-On solutions in the enterprise identity management problem space.

SAML assumes the *principal* (often a user) has enrolled with at least one identity provider. This identity provider is expected to provide local authentication services to the principal. However, SAML does not specify the implementation of these local services; indeed, SAML does not care how local authentication services are implemented (although individual service providers most certainly will).

Thus, a service provider relies on the identity provider to identify the principal. At the principal's request, the identity provider passes a SAML assertion to the service provider. On the basis of this assertion, the service provider makes an access control decision.

4.2.2.5.4 XACML

XACML[13] stands for *eXtensible Access Control Markup Language*. It is a declarative access control policy language implemented in XML and a processing model, describing how to interpret the policies. It is a replacement for IBM's *XML access control language* (XACL) which is no longer in development. Ratified by the OASIS standards organization XACML is used for defining and applying authorization policies.

4.2.2.5.5 SSL/TLS

The Transport Layer Security (TLS) Protocol [5] and its predecessor, Secure Sockets Layer (SSL), are cryptographic protocols that provide security and data integrity for communication over TCP/IP networks such as the Internet. SSL uses X.509 certificates and allows server authentication as well as mutual client-server authentication. The protocol implies encrypting algorithm negotiation, asymmetric session key exchange, message encryption using symmetric keys and message hash-signing.

The implementation of the above standards allows the realization of crucial use cases:

1. **Authentication** – Users must authenticate themselves when starting the application.
2. **Authorization** – Users must seek authorization for accessing the resources within the system.
3. **Action and resource management** – The deployment team will define the platform's available resources together with associated actions. End-users will be assigned into user roles and will be granted rights for performing actions on existing resources.
4. **Role management** – The deployment team assigns end-users of the system into user roles, thus associating the end-users with their set of allowed operations and resources.

Info World's product stack consists of complex software components that are implemented as web services using the latest Microsoft technologies such as .NET 4 and Windows Communication Foundation (WCF). Some of the most important such components are described above, as they provide crucial functionality regarding patient interaction and management of business entities and medical documentation. All the components described above are secured using the Security Services detailed in Section 4.2.2.5.

[12] http://www.opengroup.org/security/sso/

[13] https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=xacml

4.3 Use Cases Description

The present section of this deliverable describes Info World's proposed use cases for the RASEN project. The detailed processes are crucial in Info World's activity and their improvement provides the rationale for the company's involvement in the RASEN project. Each use case process is detailed as it stands today together with improvements expected from the project's implementation. The present section ends with general considerations regarding the expected medium and long term effect of the RASEN implementation across crucial Info World processes.

4.3.1 Targeted Processes within Info World

This section details those organizational processes that Info World expects to benefit most from the RASEN implementation. These are the process for the implementation of new features in Info World's eHealth software and the internal security testing process that all products must go through.

4.3.1.1 Development of New Features

The present section describes Info World's first use case for the RASEN project which concerns the development of new features within Info World's targeted software systems.

4.3.1.1.1 Description of Current Process

Due to the technical complexity of the provided software components, the implementation of new features is considered a complex undertaking, but one that follows a well-known sequence of steps that is initiated when the new feature is first proposed.

Many stakeholders can advance a proposition for the inclusion of a new software feature. For instance, management may feel that it would provide an edge for the company's product on the home market or abroad. Representatives of the sales department can request new features that allow for a better positioning of the product when compared to existing competitors. The deployment team that is in constant contact with the end-user (e.g. hospital and clinic medical staff) has relevant information about how the products are actually used and by whom and is in a prime position to request changes. Last but not least, some required features are identified directly by the development and testing teams and proposed directly by them.

The next step involves the analysis and design phase for the proposed feature, which is undertaken by the relevant research and development team. This step is crucial as it must address some well-known issues that are relevant to RASEN:

- **Existing domain standards** – Does the new feature require using some standards that were not used within the product stack before? If the answer is affirmative and multiple such standards exist, one must be selected with regards to compatibility with the company's products, ease of implementation together with aspects regarding security and confidentiality of data. More so, employed standards must be legally compatible with the legislation of the countries where they are to be employed.
- **Security Issues** – Is the new feature properly secured using the existing infrastructure? If not, additional analysis must be performed to identify the necessary means of providing security and confidentiality to the new features, both from technical and legal standpoints.
- **Compliance Issues –** Is the proposed implementation compliant with existing (and future) legal norms regarding security and protection of users' private data?

Name (ID)	New Feature Implementation Process (IW_RSL_1)
Category	Risk assessment, Security Issue, Legal Issue
Brief Description	This a complex multi-step process employed for the implementation of new features in Info World software.
Purpose/ Requirement	The purpose of this use case regards the development of secure and confidential software systems, achieved by employing risk analysis and undertaking risk based security testing activities.
Primary Stakeholder	Software development team Software testing team Security testing team
Narrative description	The steps of the feature development process are: 1. Requirement of new feature (deployment team, management team, development team, ...) 2. Analysis and design of the approved feature including an informal risk assessment step. 3. Implementation of the feature within the product by the programming team 4. Nightly build (Automated) 5. Smoke testing (Testing team) 6. Monthly build (Automated) 7. Build testing (Testing team)

Table 5 – New feature implementation

After the analysis phase is completed the feature is moved into the implementation phase where the relevant software artifacts are created and added to the existing code repository.

Checked-in source code is compiled every night as part of the company's nightly build process, so that each feature is testable within the entire application context the following day.

This approach was designed as Info World's policy of quick adaptation to changing requirements that allows providing clients with quick updates and important features in a short time span.

After the implementation of a feature, it is moved to the testing phase that is described in Section 4.3.1.2.

4.3.1.1.2 Scenario Regarding New Feature Implementation

The software systems detailed in Section 4.2.2 sit at the bottom of Info World's product stack. They are designed in a modular fashion that enables high-level functionality applications to be built on top of them to provide complex functionality to system users. One of such systems is the aFine platform for medical form design and execution, which is currently used across high-level Info World products implemented both using the desktop and online paradigms. As such, the security and confidentiality provided by the services detailed in the previous Section must translate without loss to these higher order systems to ensure flawless functioning of delivered applications.

As shown in Figure 5, the software systems detailed in Section 4.2.2 are used to implement basic functionality within the aFine platform: medical templates are stored using the RLUS component, while the EVS service is tasked with management of clinical vocabulary used throughout the form system.

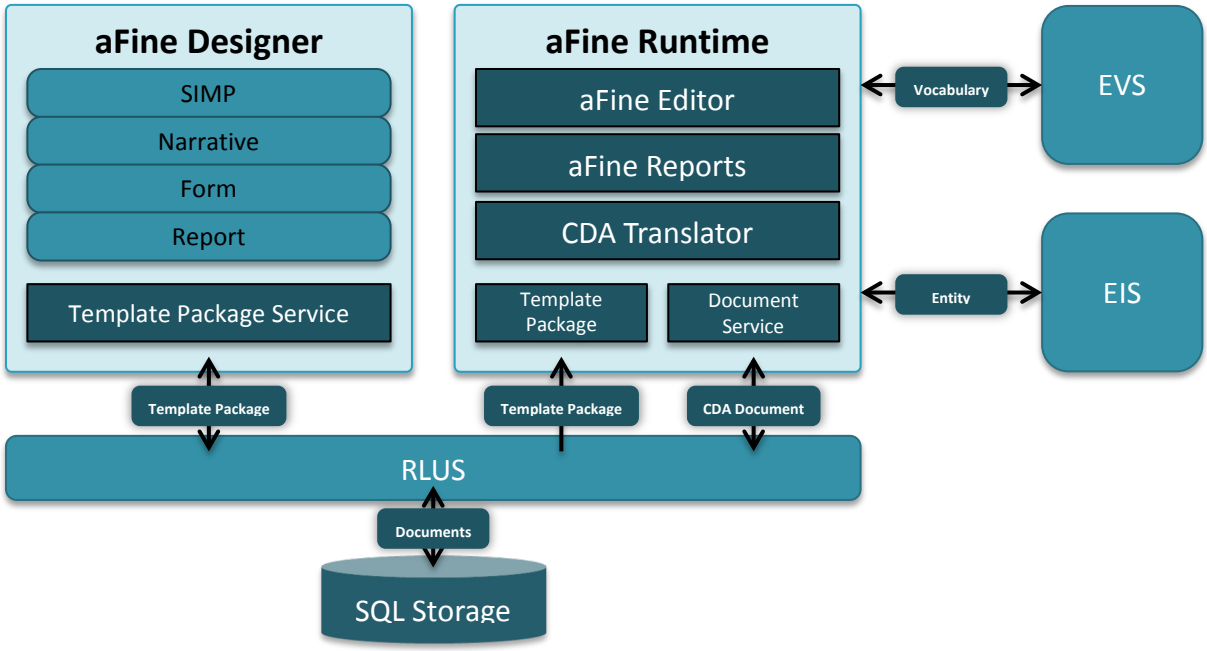

Figure 5 – aFine platform architecture

As many medical forms work with medical organizations and refer medical personnel and patients, access to the EIS service is also required.

Due to the changing nature of health legislation in Romania, coupled with the diversity of Info World's client organizations, new medical forms or changes to existing ones are frequently requested by clients, most often via the company's deployment team. Figure 6 details the process of implementing a new feature or change within the aFine medical form platform. In details, the steps are as follows:

1. The client, usually via the deployment team requests a change in an existing form or requires the implementation of a new medical form.
2. The Clinical Document Architecture (CDA) documentation that formally details the HL7 message format used by Info World is updated if required (usually when new vocabulary codes are required).
3. Existing templates for HL7 documents are updated if required.
4. The new/updated forms are implemented by the development team using the aFine Integrated Development Environment, which are then passed to the testing team where they are required to pass a rigorous functional testing phase.
5. The new/updated forms are evaluated by the client and deployed within their workflows when considered suitable.

Built using .NET 4 and Silverlight, the aFine platform was designed to enable the creation and use of cross-platform medical forms that are accessible from all Info World systems. Parts of these systems are built as complex networked desktop applications while others are rich web applications built using Silverlight technologies and integrated with in-house Java components. The pervasiveness of the aFine platform within the high-level solutions requires it to adhere to high standards of security and confidentiality.

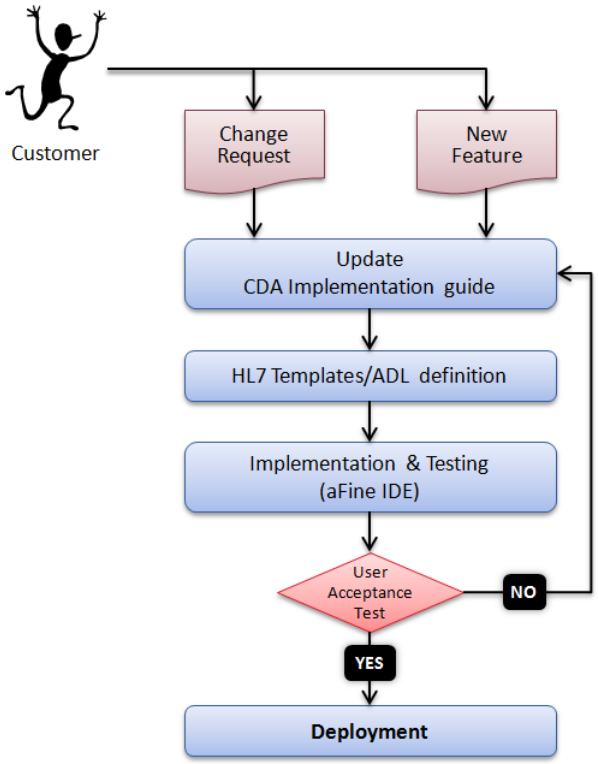

Figure 6 – Customer Change Request for aFine

Like individual software components and services, the aFine platform undergoes regular functional and non-functional testing, including security-oriented testing. However, the process of new feature implementation does not include any formal risk assessment or targeted security testing activities, making the resulting artifacts susceptible to security and confidentiality issues arising from individual components. Even more so, since these higher-level platform components aggregate functionalities provided by lower level systems they present the specific risk of aggravating existing vulnerabilities by composition of vulnerable systems. While these risks are known within Info World, the efforts of mitigation are at present ad-hoc, informal and entirely based on the technical expertise of the development and security testing teams.

A formal risk assessment step should be integrated within the feature development process at the earliest feasible stage as this would allow undertaking a formal analysis of all known risk factors, taking into account the specific systems used within the platform and creating a global risk picture by aggregating known information about all the individual system components.

4.3.1.1.3 Desired Improvements

The feature development process is one of the crucial processes within the company, as it guides the technical aspects of the provided products' evolution. The most desired improvements to the development process regard the integration of formal risk assessment within the process both for assessing the security and confidentiality of data as well as for compliance/certification reasons.

Section 4.3.1.1.2 provides an example of how the base services detailed within Section 4.2.2 are used in conjunction to provide higher-level functionality for end-users. While not an independent component in itself, the aFine platform is integrated within most of Info World's solutions for end-users and thus forms a critical part of the available infrastructure. A formalized risk assessment process tailored to the requirements of the aFine platform will allow an early analysis of risks and vulnerabilities and can be used to guide the development of new features within aFine and to better target the testing process which is detailed in Section 4.3.1.2.

By generalizing the aFine scenario presented in Section 4.3.1.1.2, a formal risk assessment methodology that is tightly integrated with the development process can be relied upon to mitigate

security and compliance risks and in the long run enable cost savings by detecting possible security issues at the earliest possible time and can provide valuable information about the risks faced by the company's product portfolio regarding compliance/certification issues. As Info World is not only an international supplier of eHealth solutions but an active participant in the development of several EU research projects expected to provide working software solutions it is important to have a comprehensive analysis regarding compliance of the offered products as soon as possible. A new methodology can be of great help, especially if it is designed from the start with such concerns in mind.

Of course, Info World's initial assessments show that integrating such a complex analysis within existing processes is a complicated task, so a working solution is expected to be implemented within 2 years after the RASEN project's successful completion.

4.3.1.2 Security Testing

The present section details Info World's current process for security testing its software together with expected improvements enabled by the adoption of the tools and methodologies resulting from the RASEN implementation.

4.3.1.2.1 Description of Current Process

Info World employs a multi-layer testing process designed to catch faults at the earliest point in time in order to enable their quick resolution. Of course, the process also integrates security testing designed to reveal security related faults and vulnerabilities.

The first step of the process is smoke testing. This is performed every day using the last nightly build by the testing team. Solving smoke testing problems is always a high priority task to make sure that the latest version of the application is always available and usable. Smoke testing has no security-testing component.

The second phase of testing consists of build testing. At the end of each development cycle lasting around one month, a new build is usually released and goes through complex functional and non-functional testing that also includes security testing. Current processes divide security testing into two areas that are usually handled by two different teams:

Functional testing – This process falls into the responsibilities of the testing team. Focus is placed on the components of the Security Service itself, especially the parts relevant for Authentication and Authorization of the system's users. Existing batteries of tests contain scenarios aimed at gaining confidence in the security of the provided solution stack.

More specifically, some of the issues that undergo functional testing include:

- Only users having valid credentials are allowed to Authenticate.
- The Authorization process works correctly in allowing access to defined actions/resources for authorized users.
- User groups are allowed the correct level of access to available functionality.
- All available actions and resources are correctly attributed to user roles.

Vulnerability testing – This procedure is undertaken by the programmers from Info World's security team. It includes both passive testing (monitoring of inter-component messages) and active testing by creation and execution of test cases. This process is used to check for vulnerabilities, especially within components secured using WS-Security, WS-Trust, SAML and XACML to ascertain the correct implementation of the above mentioned technologies.

The main hurdle in the way of security testing is the complexity of the process itself. Security testing represents a wide-ranging array of concepts and procedures making it next to impossible to fully cover all existing aspects in terms of security vulnerabilities using traditional testing patterns. The current security testing procedures mostly rely on verifying that positive requirements, or limited negative requirements, are met. The focus is mostly put on the Authentication and Authorization components, with limited vulnerabilities testing, because of the increased complexity of testing negative requirements by transforming them to a large aggregate of positive circumstances – even impossible in some situations.

The difficulty of testing complex software systems is one of the key reasons for Info World's involvement in the RASEN effort, as new methodologies and tools that aid with security testing and the formalization of risk assessment are expected to yield important improvements to existing processes.

Name (ID)	Security Testing Process (IW_SL_2)
Category	Security Issue, Legal Issue
Brief Description	This a complex multi-step process employed for the risk analysis and security testing of Info World products.
Purpose/ Requirement	The purpose of this use case regards the discovery of security related issues in Info World software, together with identifying relevant risks by performing risk analysis.
Primary Stakeholder	Software testing team Security testing team
Narrative description	The steps of the security testing process are: 1. Functional testing (Testing team) 2. Vulnerability testing (Security team)

Table 6 – Security testing process

4.3.1.2.2 Scenario for Security Testing

Due to Info World's domain of activity, all implemented solutions must undergo thorough security testing to ensure that delivered products are suitable for processing confidential patient data. However, security testing complex networked systems that have evolved over many years of development and underwent several platform changes is no trivial task. The present section provides an example of a complex solution in Info World's portfolio that would benefit from the implementation of formal risk analysis integrated with comprehensively targeted security testing, namely the workflow-based platform that sits at the foundation of several implemented products such as Dashboards and InFlow.

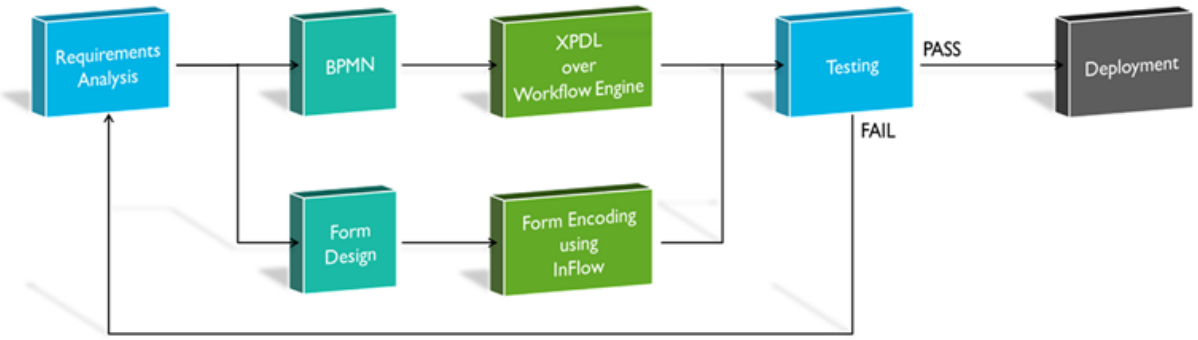

Figure 7 – Workflow-based system

Figure 7 details the business process modeling workflow that is typical for Info World solutions. The process starts with the requirements analysis, the first and most important step which may impact the correctness and performance of the final workflow. After the requirements are clearly set, the actual development of the workflow begins, with two parallel activities:

- The definition of the workflow processes using a BPMN workflow editor – which will be stored and executed as a XPDL business process definition by the Workflow Engine.
- The design of the various user input forms needed by the system, which are further encoded in an executable format.

After the design of the workflow components is completed, the user acceptance test is performed in order to decide whether the workflow satisfies the user needs, or the design process should be repeated from beginning.

Somewhat similarly to the aFine scenario contained within Section 4.3.1.1.2, the modeling process starts with a requirements analysis and ends with a testing phase right before deployment. As such, the same observations made in Section 4.3.1.1.2 still hold water: a formal risk analysis step integrated with the requirements analysis step would lead to a quicker identification of risks that will be very helpful in the context of mitigating those risks. As a main result, Info World expects the duration of the Testing phase to decrease considerably while still maintaining confidence regarding the integrity and security of the provided product.

4.3.1.2.3 Desired Improvements

Info World has employed the latest available technologies in order to secure the systems provided to its customers. Also, the company has a security testing policy that every product must go through before being shipped, as detailed in Sections 4.3.1.1.2 and 4.3.1.2.2.

However, due to the importance of securing entrusted data coupled with the possibility that at some point an attacker might actively try to access restricted systems using well known or zero-day vulnerabilities the company is committed to advancing the state of the art regarding protection of its systems.

Existing policies require testing the entire attack surface of the platform in order to gain confidence regarding the implementation. Unfortunately due to the nature of vulnerability testing itself, coupled with the complexity of the provided solutions a thorough assessment of vulnerabilities using security testing is unfeasible today. Therefore improved processes and tools are required to enable attaining the desired level of confidence.

The first step in this direction requires gaining experience with the techniques, tools and methods that will be implemented within RASEN, allowing their quick deployment and use within internal processes.

The first tangible improvements are expected within one year of the project's conclusion by integrating tools for vulnerability testing within existing security testing procedures. Due to its peculiarities vulnerability testing is a very complex procedure that requires great effort using a thorough approach. Current tools and methodologies cannot be readily adapted to Info World's use case and therefore such testing is only done ad-hoc. Another improvement regards the integration of risk assessment within the security testing process. Currently the security team only performs informal risk assessment based on security testing results and known vulnerabilities of employed technologies, which is not considered enough to ascertain the security of Info World's products. In this regard, a formalized risk assessment methodology in which all available knowledge regarding the system' implementations and known issues and vulnerabilities of the employed technology stack are employed will be much more proficient in guiding the security testing process through what is defined as *risk-based security testing*.

4.3.2 Expectations from RASEN

The main processes that are expected to see improvement as a direct result of RASEN concern the development and security testing processes. Info World expects the output of the project to enable achieving the same level of security with a significant reduction in the time required for testing. Also, the integration of formal risk assessment with the development and testing processes is expected to improve confidence in the robustness of the existing solutions, leading to an improved company image and most importantly to more secure and trustworthy systems.

During the implementation phase of the RASEN project, Info World's goal concerns gaining extensive experience in the use of techniques, tools, and methods for security risk assessment and security testing. Info World's specialists will study how vulnerability testing can be formalized and integrated into regular security testing processes. The most important identified vulnerability in Info World's security testing process concerns the lack of formalized vulnerability testing coupled with the lack of a formalized process for risk assessment. Activities within these areas are only performed ad-hoc and are completely based on the testing personnel's experience with similar software.

RASEN's output will include several state of the art tools targeting risk assessment and security testing, and current plans are in place for Info World to include these tools in its processes in order to improve the robustness and security of delivered products and to gain additional information regarding existing security vulnerabilities, their associated risk and possible compliance and certification issues with existing and future legal norms.

After an examination of current work processes Info World concluded that by adapting improved tools for vulnerability testing and improving existing processes by implementing risk assessment steered security testing the same level of product robustness and security can be achieved with a 5-10% decrease in time required for testing. In addition, a formal risk assessment strategy will provide benefits regarding the certification of existing and upcoming products and will strengthen the confidence of Info World's clients' regarding the company's product portfolio.

An additional expected benefit is the possibility of integrating the compliance/certification process with formal risk assessment. This step can be taken after Info World has a firm grasp on the integration of formal risk assessment and security testing and after reaping the first benefits of *risk based security testing*. Such integration provides cost benefits by cutting the time required for certification and enables formally proving the products' adherence to legal norms.

In conclusion, Info World expects the RASEN project to provide tools that facilitate significant improvements in processes related to low level security testing and high level risk assessment. The main beneficiaries of these tools will ultimately be the client organizations together with their end-users and patients who will benefit from complex, secure and faster-to-market applications than ever before.

5 Case Study: EVRY

EVRY is the largest IT company in Norway and the second largest IT services company in the Nordic region. With 10,000 employees, EVRY delivers daily IT services from 21 Norwegian and 50 Nordic towns and cities for more than 14,000 public and private sector customers. EVRY is the product of the largest-ever Nordic IT merger.

EVRY is a result of the merger of Norway's two largest IT companies; EDB and ErgoGroup. This was the largest merger ever seen in the Norwegian and Nordic IT industry, and was the fourth largest corporate merger in Norway regardless of industry.

EVRY is based on strong Norwegian ownership with long traditions in Norway and the other Nordic countries.[14] EVRY is listed on the Oslo Stock Exchange with the ticker code EVRY. Norway Post and Telenor are the company's largest shareholders. 1 million Norwegians use services from EVRY every day.

Over the last 10 years, the Norwegian ICT sector has grown to become the country's third largest industry. Figures published by ICT Norway show that the IT industry employs over 50,000 people and generates annual revenue in excess of NOK 160 billion.

As Norway's largest IT company, EVRY provides extensive deliveries to Norwegian and Nordic companies, financial institutions, national public sector entities, municipalities and health authorities.

According to EVRY's estimates virtually the entire Norwegian population has used IT services delivered by EVRY over the course of each week.

EVRY is responsible for about one-third of all IT services delivered in Norway, and has many customers in both the public and private sectors including such names as DnB, Telenor, Norway Post, Sparebank 1 Gruppen, Statoil, Hydro, REC, Storebrand, Gjensidige, and the City of Oslo, Trondheim municipality and the Norwegian Labour and Welfare Administration. In this project it is EVRY Financial Services that participate.

5.1 Industry Sector: Financial Domain

In banking and finance, customers rightfully expect a lot. Banks have to offer a complete, up-to-date range of services. In this market you face global competitors as well as new fast moving players. EVRY provides all IT solutions necessary to facilitate a successful bank or finance operation. You choose from a wide range of components, which EVRY in turn customize to meet requirements.

The different areas are:

Customer centric:

- Advising and sales
- Daily Banking
- Self-service Channels
- ATM Services

Cards:

- Card Issuing
- Acquiring
- Switching
- Fraud prevention
- Card production.
- Payment terminal management.

[14] http://www.evry.com/corporate/about/

- Internet Payment

Loans and finance

Payments

Savings and investments:

- traditional bank savings
- structured savings products
- combination products in banking, mutual funds and insurance
- government-regulated savings
- pension savings

Insurance

BI and compliance

Enterprise centric:

- Master Data Management
- Enterprise Content Management
- Enterprise Resource Planning
- Sales Management

Security:

- Authentication - electronic identification and single sign-on
- BankID administration-Issuing Solutions
- Electronic signing - online document signing
- Card security
- 3-D Secure Issuing - secure Internet commerce

Custom solutions

Within this project we will focus on the self-service channels. This includes net bank and the different variants of this (mobile bank, tablet bank, etc.).

5.1.1 Technical and Legal Aspects

EVRY delivers financial software to the Nordic region (banks, insurance companies, payment providers among others). As a supplier of banking and financial solutions, EVRY must ensure the solutions follow financial laws for the country the customer are in. Privacy of sensitive customer data must be fulfilled and since there are money transfers in most of the solutions, security is of importance to prevent unauthorized transactions and theft.

Poor security in these systems could lead to considerable loss for both the customer and EVRY. It can be loss of business, information leakage, loss of funds and loss of integrity.

All systems involved with payment cards (banking systems with money transactions) must fulfill the PCI-DSS standards. This is a demand from the card companies (Visa, MasterCard, etc.)

And all systems within banking and finance must be tested against OWASP ASVS (Open Web Application Security Project Application Security Verification Standard) on various levels depending on how exposed the system is.

Additionally, the banking and finance sector is regulated by law.

5.1.2 Actors

EVRY's systems are used by approximately 70% of the banking companies in the Norwegian marked. EVRY are a big actor in Sweden as well and have customers in other European countries. The users are both within the bank/financial institution as well as private persons their customers. In this project we will focus on the self-service channel, where the banks customer is the main users:

- **Private persons:** End users of net banks. These are typically the bank's customers who use the different variants of net banks to pay bills, set up budget, apply for loan electronically, balance accounts, and so on.
- **IT staff:** System administrators who are the expert for the system, IT operators who maintain the infrastructure and deploy the system.
- **Bank employees:** Via management systems they control the customer's configuration. They can send messages to the inbox and can control what the customer is authorized to access.
- **IT support (EVRY):** Can access some of the customer's information when needed to help with issues.

5.2 Relevance to RASEN

Unauthorized access, fraud and information leakage can lead to loss of money for the bank and its customer, loss of reputation for the bank and EVRY and loss of sensitive customer data.

EVRY do have an expert team for security testing and have a lot of knowledge in this area. Usually the projects in EVRY have a limited time period for security testing and would benefit from introducing risk based security testing to ensure the focus is on the most important tests for the given period of time. Introducing new test tools can be an advantage in the same area. Indirectly the results from RASEN can be used to improve the development process by giving them feedback on which high risk vulnerabilities they most frequently introduce and how to avoid them.

5.2.1 Resources involved

A description of resources involved in the RASEN project for EVRY.

- **Security testers:** EVRY has a team of highly skilled security testers which plans and executes security tests for EVRY's solutions. The main impact from the RASEN will be on the methodology for this team.
- **Developers:** EVRY expect that feedback as mentioned in 4.2 will introduce some checks to the development process to improve their output in regards to security.

5.2.2 Targeted software system

EVRY's case study is based on our self-service solutions, where we focus on the different variants of net banks. These are customer facing web applications where security is of the highest priority.

5.2.2.1 Private Net Bank.

This is EVRY's standard net bank for private customers. This solution is configured to the banks demands so they can provide internet banking for their customers. The main functions here are:

- Personal info – a bank customer can read and update personal information such as address, telephone number, etc.
- View account balance – the customer can see the balance for their own accounts
- Internal transfer – transferal of funds between own accounts, e.g. from salary account to savings account.
- Payment – transferal of funds to external accounts, e.g. pay a bill.
- Budget – a customer can set up a personal budget.

- Loan – a bank customer can calculate and apply for a personal loan.
- Transaction – overview of all transactions, both made within the net bank and transactions made with debit/credit cards.

5.2.2.2 Mobile bank

A scaled down version of private net bank targets to fit better mobile screens. It can be accessed by the mobiles web browser or via native apps for iOS/Android. Having less functionality than the standard net bank, it features the following functions:

- Personal info – a bank customer can see his personal information such as address, telephone number, etc.
- View account balance – the customer can see the balance for their own accounts
- Internal transfer – transferal of funds between own accounts, e.g. from salary account to savings account.
- Payment – transferal of funds to external accounts, e.g. pay a bill.
- Transaction – overview of all transactions, both made within the net bank and transactions made with debit/credit cards.

5.2.2.3 Tablet bank

Same as mobile bank, but formatted for a larger screen. It can be accessed by web browser or native apps.

- Personal info – a bank customer can see his personal information such as address, telephone number, etc.
- View account balance – the customer can see the balance for their own accounts
- Internal transfer – transferal of funds between own accounts, e.g. from salary account to savings account.
- Payment – transferal of funds to external accounts, e.g. pay a bill.
- Transaction – overview of all transactions, both made within the net bank and transactions made with debit/credit cards.

Both mobile bank and tablet bank needs separate security tests from net bank, because the security mechanisms differ a bit between the different platforms.

5.3 Use Case description

This section describes (1) current work processes of relevance to RASEN, (2) the areas in the current work processes where the RASEN results can be applied, and (3) the expected improvement in these areas.

5.3.1 Security testing

Current process:

The current routines of EVERY require that all deliverables shall be assessed for the need for testing and that all deliverables must be evaluated for security testing. In addition, systems must be periodically tested every 6th month.

EVRY has a dedicated security testing team. However, some security testing is performed by external companies. This is due to customer demands and PCI certification. As a standard for security testing, EVRY uses OWASP ASVS. The current testing process for pre-production is shown in Figure 8.

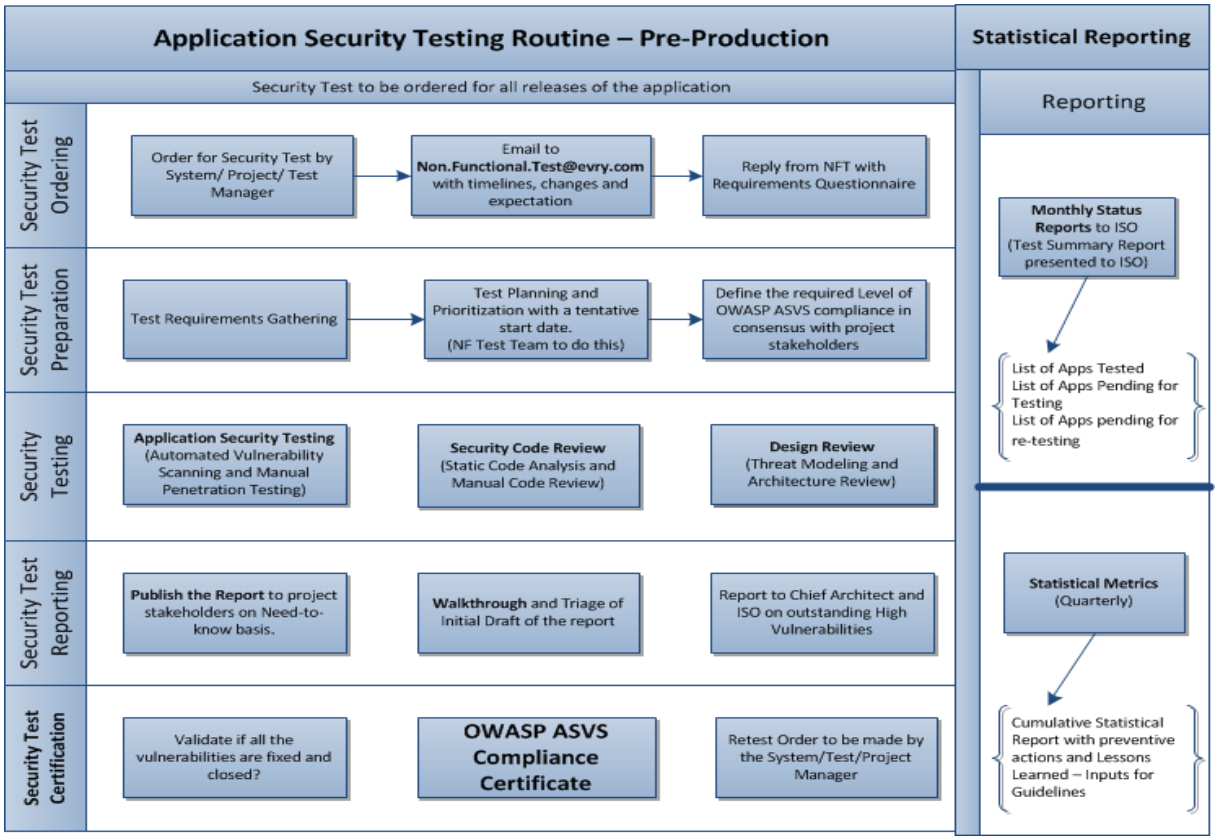

Figure 8 – Application Security Testing Routine for Pre-Production

Areas where RASEN results can be applied and expected improvements:

Since the systems can be rather complex, and usually there is limited time for security tests, the available time need to be used efficiently. EVRY don't have formal risk-based security testing today.

With the introduction of risk based security testing, the project can use the time available more effectively by using risk assessment in test planning and test the parts of the system where the risk is highest.

Additionally introduction of new tools can help improve the execution of the security tests. EVRY's expectation from RASEN is that the testing will be more effective within the given timeframe, and that the security tests focuses on the important areas of the system.

Name (ID)	Security testing (EVRY_SL_1)
Category	Security Issue, Legal Issue
Brief Description	Risk assessment in security test process
Purpose/ Requirement	The purpose of this use case is to improve security testing by introducing risk based testing.
Primary Stakeholder	Security testing team
Narrative description	The steps of the security test process are: 1. Information gathering 2. Code analysis 3. penetration tests 4. reporting 5. walkthrough 6. fix 7. retest

Table 7 – Security Testing in Financial Domain

5.3.1.1 Test and development methodology

Current process:

EVRY has no formalized security guidelines in the development methodology for secure coding. Security is of course taken care of in the design/architecture. The code itself isn't checked for security until system test, by code analysis and penetration tests. For the security testing there is a methodology (see5.3.1), but it doesn't include risk assessment.

Areas where RASEN results can be applied and expected improvements:

For the development methodology, EVRY will use the results from the risk based security testing indirectly to improve the development process. The project will see which high risk vulnerabilities that are most often repeated by the developers, and teach them to avoid introducing them.
For the security test EVRY will use the results from RASEN we think improves our testing in the methodology. EVRY will implement the methods directly into the methodology description to ensure every security tester uses the results.

Name (ID)	Development Methodology (EVRY_SL_2)
Category	Security Issue
Brief Description	Improvement of methodology.
Purpose/ Requirement	The purpose of this use case to improve development methodology by introducing risk analysis.
Primary Stakeholder	Software development team Security testing team
Narrative description	The development process hasn't got any secure coding standards. The security is tested after deployment in system test. EVRY will use the results from the risk based security testing indirectly to improve the development process. EVRY will see which high risk vulnerabilities that are most often repeated by the developers, and teach them to avoid introducing them.

Table 8 – Development Methodology

6 A Unified View of the Use Cases

This section provides a unified view across the case studies detailed by the three use case providing organizations: Software AG, Info World and EVRY. By highlighting both common and particular aspects of the described processes we lay the groundwork of a comprehensive foundation for future activities including the research phases of RASEN. This section is organized as follows: within the first subsection we provide a comparative overview of the organizations providing the project's use cases, highlighting both common and differentiating aspects. Following sections are dedicated to brief discussions regarding particular aspects within all the proposed use cases such as the presence and propensity of risk, security and legal issues, the way each of these presents itself within the use cases and their effect on the providing organization.

6.1 The Case Study Providers

The three companies that serve as case study providers for RASEN are actively developing complex software and can be considered, at heart, as software development organizations. While working in different areas (Software AG develops business software, Info World is exclusively dedicated to eHealth while EVRY provides solutions for many branches in the financial domain) the common denominator is represented by the sheer complexity of the deployed solutions; all companies provide complex network interconnected software systems that see wide use by their end users.

As detailed in the relevant chapter, Software AG is one of the fastest growing technology companies on the planet, and their deployed solutions help power businesses in diverse domains across the globe, which sets additional constraints regarding local and international legislation and regulations regarding the security and confidentiality of provided business solutions.

Meanwhile, EVRY is the largest IT company in Norway, having 10,000 employees and sees its services used by 1 million Norwegians every day. Among others, EVRY provides services to financial institutions, entities in the public sector, municipalities and health authorities. As a solution provider in the financial field, its deliverables must address issues such as identification, digital signatures, security of card usage and prevention of financial fraud.

In Romania, Info World provides eHealth services that back 4 out of 10 hospital beds managed using a software system. The security of the provided software is of paramount importance due to the sensitive nature of recorded data. As a processor of private information, Info World must abide by national and international regulations and may face stringent penalties if the security of its systems is compromised. More so, by participating in several international projects, Info World must also be knowledgeable about foreign legal systems in order to ensure the compliance of existing and future products with international norms.

The profiles, activity domains and ultimately the sheer number of end users depending on the reliable and secure functioning of the solutions represent a great responsibility on the behalf of the providers. As such, it follows that all three companies have rigorous procedures and dedicated teams for testing their products. This of course includes security testing procedures, and to some extent, management of risks.

As the RASEN project is focused on security aspects of software, the present document is also weighted towards issues relating to security, confidentiality and privacy. The three case study providers have a stated common interest of providing highly secure and reliable systems. Failure to do so is commonly identified by all parties to result in loss of revenue, loss of reputation together with costly lawsuits or heavy fines and restrictions imposed by national regulatory bodies.

The following sections are used to present common issues and challenges faced by the described use cases and to highlight the peculiarities of each scenario presented in the course of the preceding chapters. The provided information synthesizes the current state of processes which are established at the three organizations while highlighting industry specific aspects. As such, the present section can act as a rough starting point for defining the requirements for the research phases of the RASEN project.

6.2 Risk issues

This first subsection provides a global overview of how risks pertaining to the security of the delivered solutions are currently managed within the three providing organizations.

Formal risk assessment is part of Software AG's development process, but is currently undertaken only for products that have shipped or are ready for shipping, which makes issues discovered in this phase very expensive and time consuming to solve. With regards to the implementation of RASEN, Software AG has expectations regarding the possibility of shifting the risk assessment phase to an earlier stage of the process where uncovered issues could be mitigated quicker.

Meanwhile, providers Info World and EVRY employ an informal risk assessment process based mainly on the experience of the security testing teams that are employed within each company. While having a direct feedback from highly-skilled personnel can be a fundamental asset in security testing, both partners express a strong desire to also integrate a formal risk assessment process within their development and security testing workflows.

By perusing the RASEN use cases we can observe a common theme that permeates across all provider organizations. First of all, if not already in place, organizations understand the importance of formalized risk assessment and desire to implement it within their development and testing processes. Second of all, the importance of well integrated risk management is clearly pointed out: when discovered earlier in the production pipeline, issues such as security vulnerabilities, bugs, errors and so on can be mitigated quicker and significantly cheaper.

Also, a common issue among the case study providers regards the unification of models that are obtained using risk assessment and testing. Generally, risk assessment provides a high level view of a product, while testing results reveal pinpoint faults within the system. Finding a common denominator to aggregate these views remains an open question in research and is one of the goals of RASEN. Related to this problem is what is called *risk-based security testing*, namely the guidance of the security testing process using the results of a formalized risk analysis. The development of a practical methodology, backed by industry-ready tools for implementing it is one of the goals of RASEN that is expected by all three case study providers.

The existence of such a toolset, usable by all three providers in the development of commercial products will be one of the main long-term benefits of RASEN, leading to shorter times-to-market and a decrease in the effort associated with testing for a broad class of applications.

6.3 Legal Issues

All case study providers presented in the current deliverable develop highly complex solutions for handling critical customer data. Software AG's vast product portfolio covers a wide range of business solutions that are used world-wide by client organizations involved in many areas. EVRY's solutions are oriented towards the financial sector in the Nordic region. With an estimated 1 million daily users EVRY's products must ensure the strictest adherence to existing legal norms in order to ensure complete protection of the end-user's financial data. Similar issues are encountered by Info World, who process highly sensitive patient data in Romania and abroad. For all the detailed systems there exist international and national laws and regulations that providing organizations must strictly abide. Failure to do so might result in loss of confidence and further fines and restrictions from national regulatory bodies.

Of course, the exact norms and regulations depend on the case study provider's field of activity. Software AG products must adhere to the *Common Criteria for Information Technology Security Evaluation (ISO 15408)* standard which defines a common criteria framework used to specify functional security and assurance requirements of IT products and computer systems. More so, for systems deployed within the US there exist separate requirements from the NIST[15] that are available in several FIPS[16] documentations such as *FIPS PUB 200, FIPS PUB 140-2, FIPS PUB 180-4* and many others. Compliance with these norms is mandatory for US operation, therefore solution providers face the additional task of ensuring their products comply with existing regulations. More so,

[15] National Institute of Standards and Technology
[16] Federal Information Processing Standards

existing products that are deployed long-term must be updatable to newer security and confidentiality standards whenever they become available.

Rigorous standards also exist for financial applications. As such, EVRY products are thoroughly tested both in-house and by external entities to ensure stringent requirements for security testing specified in the *OWASP ASVS*[17] are met. More so, EVRY solutions are *Payment Card Industry*[18] certified to ensure reliable operation.

The main legal concern for Info World regards the processing of highly sensitive patient information. The relevant international regulation regarding the protected handling of personal data is contained in the *95/46/EC Data Protection Directive*. The Directive is not legally binding for citizens and thus has to be transposed into law by all EU countries; the relevant Law for Romania is 677/2001. This also lead to the creation of a national regulatory body called the National Authority for the Oversight of Processing of Personal Data that created more specific norms that have to be obeyed by personal data processors. As Info World also operates within other EU countries and even for clients outside the EU, there also are other norms to consider.

The wide array of legal regulations that cover the activity domains of the three case study providers represents a real challenge for the RASEN project. However, a formalized procedure that would simplify the compliance/certification process would greatly help provider organizations by considerably lowering the costs associated with creating products used across the globe, an issue commonly identified in all descriptions of current use cases.

6.4 Security Issues

The security of the solutions offered by the case study providers is of paramount importance. While Software AG products form the backbone of many solutions in different fields, EVRY and Info World provide more targeted solutions for financial and health systems, respectively. The common denominator among all providers is the stringent need for securing the deployed systems against existing vulnerabilities, software bugs and malicious users or external hackers.

All organizations recognize the importance of securing their products and have taken important steps towards that goal. In this respect, they can be considered as adopters of the newest tested security technologies. However, as they all attest, security testing is a very complex undertaking due in part to the complexity of the developed systems and in part to the high value that a malicious user would ascribe to discovering an exploitable security issue within one of the systems.

In order to mitigate existing risks, thorough security testing is undertaken by each of the partners using specialized personnel and an agile approach that sees software built and tested every day. For instance, Software AG employ automated source code and binary code scanners in their development methodology to identify issues, including security issues as soon as source code is checked in. In addition, software goes through a gauntlet of testing phases: unit testing is followed by integration testing between built components and finally penetration testing where the security and resilience to attack are put to the test.

For their financial applications, EVRY employ an internal security testing team that use well known guidelines within their activity and create detailed reports regarding the discovered issues. A strict process for security testing is in place that ensures that deployed applications conform to the OWASP ASVS standards. More so, the security testing team is strictly divided from the development team to ensure independent operation and a lack of influence between them. As financial applications have to comply with existing legal standards some of the security testing is performed by external entities in order to increase end-user confidence and to ensure PCI certification.

The product stack developed by Info World is also security tested by an internal testing team; major efforts are geared towards functional security testing and vulnerability testing, with accent placed on components for Authentication and Authorization. This is especially important in Info World's case to ensure that no unauthorized access to the secured systems take place. This may happen from the exterior, using known or zero-day vulnerabilities or from the interior, when an authenticated user gains

[17] Open Web Application Security Project Application Security Verification Standard
[18] https://www.pcisecuritystandards.org/

access to areas of the system that should be restricted for them. Within Info World security testing is undertaken by the testing team and is usually performed when a new build of the platform is released, which usually happens every month.

The common issue facing the case study providers is the sheer amplitude of security testing complex networked products. By having multiple entry-points within the system these solutions present rather large attack surfaces that need to be secured. The main identified expectation from RASEN is a methodology for *risk-based security testing* that would allow targeting the security testing process over areas that are considered vulnerable or at the highest risk. Such a methodology would lessen the importance of individual testers' skills and would eliminate the need for "carpet bombing" as a security testing methodology by focusing creation and execution of test cases on the critical areas of the applications.

Another important issue regards the secure development of code. While security is a front matter concern for the case study providers, neither of them implement strict guidelines for the implementation of secure code, relying on the testing phase to identify issues. While not of direct concern to RASEN, formal guidelines for secure code development, possibly guided using risk management techniques could lower development costs and lessen the effort required for security testing.

6.5 Use Cases Discussion

This subsection examines the case study provided by Software AG, EVRY and Info World for the RASEN project. Common challenges were identified across the four use cases and particular issues were outlined and discussed.

A first observation that can be made is that all three organizations arrived to rather similar processes for developing software solutions, even though their expertise is not focused on a single area. This gives hope that the solutions identified within the research phases of RASEN will be equally applicable across many application domains.

A second issue regards the complexity of security testing. As the world relies more and more on software systems, organizations take up the challenge to deliver reliable and secure systems to customers. However, we face crucial issues regarding the security and confidentiality of the delivered systems. In general, security testing is an open domain for research where significant advances are still possible and highly desirable. In this tone, the RASEN project's goal is to advance the state of the art in a commercially viable way that will enable beneficiaries to see the immediate benefits of the newly developed tools and methodologies.

The last but not least issue regards risk assessment. While as an informal activity it is undertaken within all three organizations and formalized within one, there exists the need for a more formalized approach that is better integrated within the development process and that allows for the creation of testing artifacts to improve upon the security of the delivered solutions.

As can be seen in the present Section, the use cases provided by the three partners cover important processes within each organization and present significant challenges for the research and technology partners. The implementation of new tooling, together with an associated methodology would greatly benefit not only the participating organizations but also others, as the results are expected to be widely usable across many organizational processes.

7 Conclusion

Work Package 2 of the RASEN project aims to clearly define the three case studies that will be used to assess and validate the RASEN approach. To this end, the consortium includes three distinct organizations that build and deploy software as a significant part of their activities. The chosen organizations build complex software that processes data from millions of users every day and has important requirements with regards to the security of the solution and privacy of the processed data. In this context, the present document aims to detail those processes within each of the organizations that are to be targeted and improved by using the RASEN approach. Also, the present document provides a thorough overview regarding key processes within each of the organizations together with a description of the common and distinct aspects of these processes.

Section 2 of the document provides a high level overview of the project's use cases, detailing the most important aspects targeted by the RASEN project. Also, Section 2 is used to identify relevant stakeholders for each of the proposed use cases together with the characteristic risks identified for each of them.

The following three sections of the document introduce the three case studies in detail. Section 3 presents Software AG's business software development process and details the relevant use case. Within Section 4, Info World's use cases are detailed regarding the eHealth field. They consist of the implementation of new features within the existing software stack and the security testing of existing products. Section 5 is dedicated to EVRY's case study. As an important financial player within the Nordic countries, EVRY's systems process a significant portion of all e-payments occurring within the market and as such their security is paramount.

Section 6 of the document provides a brief comparative overview of the use cases from the three companies. In particular, risk issues, security issues and legal issues are discussed with regards to how they pertain to each of the presented use cases.

The present deliverable is the first part in the work outlined for WP2. From the basis established in the present document the project's requirement must be defined and use case studies conducted. Furthermore, future work will include two phases of use case study evaluation to assess the progress of the RASEN project.

The case study providers in the RASEN project have a diverse operation base and have different experience with use of risk analysis in their organizations. All partners have a clear idea on how this project can contribute to improve key processes within their organizations. Since the partners come from different industries, their views on the project and expectations also have differences but crucial themes are mentioned by all partners (e.g. risk analysis in the security testing process). This is a good indicator of the fact that unified processes and tools would be useful to all of the partners involved and thus can be applicable in a broader scope of other enterprises in Europe. We believe this to be a good motivator for the research work within the RASEN project which we believe the project can provide important improvements regarding the state of the art in the domain.

Glossary and Abbreviations

ADT - Admission, Discharge, Transfer Service

B2B - Business to Business

BPMN - Business Process Management notation

CDA - Clinical Document Architecture

CRUD - Create, Read, Update, and Delete

CTS - Common Terminology Services

DBMS - database management systems

DoS - Denial of Service

EAL - Evaluation Assurance Level

ECHR - European Convention on Human Rights

EIS - Identification Service

ERP - Enterprise Resource Planning

EVS - Enterprise Vocabulary Service

FIPS - Federal Information Processing Standard, United States government standards

HIS - Hospital Information System

HL7 - Health Level v7

HSSP - Healthcare Services Specification Project

ICT - Information and communications technology

ISO - International Organization for Standardization

MMC - Microsoft Management Console

NIST - National Institute of Standards and Technology

NPL - Natural Programming Language

OID - Object Identifier

OWASP ASVS - Open Web Application Security Project Application Security Verification Standard

PP - Protection Profile

RIM - Reference Information Model

RLUS - Retrieve Locate and Update Service

SAML - Security Assertion Markup Language

SAR - Security Assurance Requirement

SFR - Security Functional Requirement

SHS - Secure Hash Standard

SOA- Service Oriented Architecture

SSL - Secure Sockets Layer

SSO - Single Sign-On

ST - Security Target

TLS - Transport Layer Security

TOE - Target of Evaluation

XACL - XML access control language

XACML - eXtensible Access Control Markup Language

XPDL - XML Process Definition Language

References

[1] The European Commission's Data Protection Directive Number 95/46/EC, Official Journal L 281, P. 0031 – 0050 (1995) [ONLINE] Available at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML [Accessed 23 January 2013]

[2] The European Union Data Protection Regulation [ONLINE] Available at http://ec.europa.eu/justice/newsroom/data-protection/news/120125_en.htm [Accessed 22 January 2013]

[3] H. R. Kensaku - Healthcare Services Specification Program, 2009 [ONLINE] Available at http://www.ncbi.nlm.nih.gov/pmc/articles/PMC3002132/, [Accessed 20 December 2012]

[4] Health Level 7 Common Terminology Services [ONLINE] Available at http://wiki.hl7.org/index.php?title=CTS [Accessed 23 January 2013]

[5] T. Dierks, C. Allen - The TLS protocol (1999) [ONLINE] Available at http://www.ietf.org/rfc/rfc2246.txt [Accessed 20 December 2012]

[6] ISO 15408, Information technology -- Security techniques -- Evaluation criteria for IT security (2009)

[7] John E. Bryson, SP 800-53 Rev. 4, DRAFT Security and Privacy Controls for Federal Information Systems and Organizations (Initial Public Draft), National Institute of Standards and Technology (2012)

[8] Patrick D. Gallagher, NIST Special Publication 800-132, Recommendation for Password-Based Key Derivation, National Institute of Standards and Technology (2010)

[9] Karen H. Brown, A Comparison of the Security Requirements for Cryptographic Modules in FIPS 140-1 and FIPS 140-2, NIST Special Publication 800-29 (2001)

[10] Elaine Barker and Allen Roginsky, Transitions: Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths, NIST Special Publication 800-131A, Computer Security (2011)

[11] Elaine Barker and John Kelsey, NIST Special Publication 800-90A, Recommendation for Random Number Generation Using Deterministic Random Bit Generators, Computer Security Division, Information Technology Laboratory (2012)

[12] Karen Kent and Murugiah Souppaya, Guide to Computer Security Log Management, Recommendations of the National Institute of Standards and Technology, Special Publication 800-92, NIST (2006)

[13] Patrick Gallagher, DRAFT FIPS PUB 180-4,Secure Hash Standard (SHS), Information Technology Laboratory, National Institute of Standards and Technology (2011)

[14] Carlos M. Gutierrez , FIPS PUB 200, Federal Information Processing Standards Publication, Minimum Security Requirements for Federal Information and Information Systems, National Institute of Standards and Technology (2006)

Appendix A: Use-Case Scenario Template

This part gives detailed information regarding the structure of the use cases template with respect to structure and requirements.

Use Case Name

Each scenario is associated with a unique name suggesting its purpose. The name expresses what happens in the scenario under consideration. It is recommended that the name is an active phrase that includes active verb and a noun.

Use Case ID

A unique identifier is assigned to each use case. The identifiers follow a specific naming which indicates e.g., the scenario in which the use case is relevant. It further provides a hierarchical relationship between the use cases to build clusters.

Example:

- *R1 for the 1st Scenario addressing Risk Assessment*
- *L2 for the 2nd Scenario addressing Legal Issues*
- *S5 for the 5th Scenario addressing Security Issues*
- *Other (maybe we need to extend the categories here!)*

Category

This property relates the given scenario to a specific group which enables comparisons and a better clustering for the upcoming analysis. Possible categories are

Example:

- *Risk Assessment*
- *Legal Issue*
- *Security Issue*
- *Other (May need an extension of the categories!)*

Brief Description

This field provides a brief description of the reason for and outcome of this use case or a high-level description of the sequence of actions and the outcome of executing the use case scenario. Use at most 2 sentences and the more precise the formulation the better.

Purpose/Requirement

The purpose of this task is to describe use-case scenarios in sufficient detail to validate understanding of the requirements, to ensure concurrence with stakeholder expectations, and to permit further development to begin.

Primary Stakeholder

Stakeholders or actors are either persons or systems which play a key role for the scenario. Each stakeholder defines a coherent set of roles that it can play within the use case scenario. A distinction can be made between primary and secondary stakeholders if needed. A primary stakeholder is the one having a key role in the scenario definition where as a secondary stakeholder is optionally and possibly depending on the situation.

Example: Risk Manager, Customer, etc.

Narrative description

This field provides a listing of the use case scenario in in more detail using natural language.

Use Case Template

The Use Case Template as displayed in the following should be used to structure the different scenarios which partner contribute and make them better readable, comparable and understandable for up-coming tasks.

Name (ID)	Name of the Use Case Scenario (ID)
Category	[Risk Assessment, Legal Issue, Security Issue]
Brief Description	This field provides a brief description of the reason for and outcome of this use case or a high-level description of the sequence of actions and the outcome of executing the use case scenario. Use at most 2 sentences and the more precise the formulation the better.
Purpose/ Requirement	The purpose of this task is to describe use-case scenarios in sufficient detail to validate understanding of the requirements, to ensure concurrence with stakeholder expectations, and to permit software development to begin.
Primary Stakeholder	Which parties are involved? S1 S2 (Optional 2nd Stakeholder)
Narrative description	This field provides a listing of the use case scenario in in more detail using natural language.

Table 9 – Use Case Template