BULGARIAN ACADEMY OF SCIENCES
INSTITUTE OF INFORMATION AND
COMMUNICATION TECHNOLOGIES

TODDOR VELEV VELEV

MODELING AND AUTOMATION OF STANDARDIZED INFORMATION SECURITY MANAGEMENT SYSTEMS

ABSTRACT OF PhD THESIS

for acquiring the educational and scientific degree
"doctor"
in the doctoral program in the scientific specialty
"Informatics"
professional field 4.6 Informatics and computer science

SUPERVISOR: PROF. DR. NINA DOBRINKOVA

Sofia, 2025

The dissertation was discussed and admitted to defense at an extended meeting of the "Modeling and Optimization" section of IICT-BAS, held on .....2025.

The dissertation is structured in an introduction, three main chapters, main conclusions and inferences, appendices, and a comprehensive list of references. The total volume of the dissertation without appendices is 124 pages, which includes rich illustrative content of 29 figures (diagrams, schemes, screen shots) and 34 tables presenting data and classifications. The list of references contains 80 sources, demonstrating the breadth and depth of the literature review conducted.

The defense of the dissertation will take place on ……. at …… hours in hall …… of block …… of IICT-BAS at an open meeting of a scientific jury composed of:

1. …….
2. .....
3. .....
4. .....
5. .....

Reserve members:

1. .....
2. .....

The materials for the defense are available to those interested in room …. of IICT-BAS, ul. "Akad. G. Bonchev", bl. …..

Author: Todor Velev Velev
Title: MODELING AND AUTOMATION OF STANDARDIZED INFORMATION SECURITY MANAGEMENT SYSTEMS

I. GENERAL CHARACTERISTICS OF THE DISSERTATION

Relevance of the problem

In the modern information reality, characterized by the dynamic digitalization of all social and economic processes, information is becoming a strategic asset and at the same time an increasingly vulnerable resource. The daily exchange of huge amounts of data, the complex infrastructure of interconnected systems and the widespread use of cloud technologies and mobile devices lead to an increase in threats to information security. Cyberattacks, incidents of unauthorized access and data compromise are becoming more frequent, which poses challenges to organizations, both in the public and private sectors.

Traditional approaches to security, based primarily on manual processes, separate technical means or formal implementation of minimum requirements, no longer meet current risks. Against this background, international standards, such as ISO/IEC 27001, NIST, FISMA, GDPR and others, require a systematic, integrated and adaptive approach to information security management. They imply the construction of information security management systems (ISMS) that combine policies, procedures, technologies, human factors and organizational culture.

Automation of processes in ISMS is a new necessity, predetermined by the complexity and volume of data and information flows. Digital ISMS management platforms must

provide traceability, control, continuous assessment and improvement, as well as the ability to integrate with new regulatory requirements and business changes. In this dynamic environment, information security is a task of high priority and increasing importance. Information security management systems are not adequate without automated platforms with elements of artificial intelligence to master the growing volume and types of information flows and interactions.

The relevance of this dissertation stems from a clearly identified need for a new, qualitatively different approach to the management of standardized SMIS. This approach should be based on a formalized, semantically rich model of the security domain and use this model to achieve a high degree of process automation. The development of an intelligent, integrated software environment (platform) based on such a model can dramatically increase the effectiveness, efficiency and adaptability of security management, while reducing costs and administrative burden on organizations.

Object and subject of the study

The object of research is standardized information security management systems (ISMS) and the possibilities for automation of functionalities and their management.

The subject of research is a Model of a software product, a complex Platform, that can model and automate any information security management system, built in accordance with an internationally recognized standard or standards in this field.

Goals and objectives

The goal of the dissertation is to develop and validate a platform model to manage and automate standardized information security management systems.

To achieve this goal, the following tasks have been formulated:

- Research and analysis of the theoretical foundations of standardized information security management systems in aspects:
  - Information security;
  - Information security standards;
  - Information Security Management Systems (ISMS);
  - Software applications for IS.
- Analysis of the processes, requirements and characteristics of the platform for management and automation of standardized information security management systems. The task is divided in accordance with the specified methodology into the following subtasks:
  - Research and analysis of work processes subject to automation and their corresponding information flows;
  - Determining the functional and non-functional requirements of the platform, through research and analysis of data, user groups and information security standards;
  - Identifying the general characteristics of the system.
- Design of an optimal platform model for modeling and

automation of standardized information security management systems and its associated architecture.

Methods

To achieve the goals and objectives set in the dissertation, a combination of research methods was used, ensuring both theoretical depth and practical applicability of the results.

- **System analysis**

This method was applied to consider the ISMS as a complex, dynamic system of interconnected components, processes and activities. Through the systems analysis, the main elements of the ISMS, their dependencies, input and output parameters, as well as their interaction with the external environment of the organization were identified. The systems approach allowed for the structuring of the problem, its decomposition into smaller, manageable parts and their integration into a single platform model.

- **Comparative analysis**

An in-depth comparative analysis of various international standards (ISO/IEC 27001, ISO/IEC 27002, NIST Cybersecurity Framework), regulatory requirements (GDPR, NIS2), risk management methodologies (ISO 31000) and existing software solutions for ISMS was carried out. This analysis allowed the identification of good practices, common elements and gaps in current approaches, which served as the basis for formulating the requirements for the new platform.

- **Modeling**

The modeling method is central to the dissertation. The following techniques were used:

  - Conceptual modeling - for high-level definition of the components and logical structure of the proposed platform;
  - Architectural modeling - for designing the software architecture, including the selection of layers, modules, and technology stack;
  - Business Process Modeling (BPMN - Business Process Model and Notation) - used for a detailed description of key processes in an information security management system (e.g. risk assessment, incident management, audit) for the purpose of their standardization and preparation for automation;
  - Data modeling (ERD - Entity-Relationship Diagram) - is used to structure information, define objects, their attributes and relationships necessary for the platform's database.

- **Data analysis**

Used to collect, systematize, process, and interpret information related to cyber threat statistics, effectiveness of existing security measures, as well as data generated during prototype testing.

- **Literature review**

A thorough and systematic review of scientific and professional literature was conducted - books, scientific articles, conferences, reports, standards and good practices in the fields of

information security, management systems, process modeling, software engineering and automation.

- **Expert assessment method**

When defining the requirements and validating the model and prototype, expert opinions and recommendations from specialists in the field of information security and auditing were indirectly taken into account. The combination of these methods provides a comprehensive approach to the problem, combining theoretical knowledge with practical application and validation of the proposed solutions.

II. VOLUME AND STRUCTURE

The dissertation is systematically organized into an introduction, three main chapters, main conclusions and inferences, appendices, and a comprehensive list of references. The total volume of the dissertation without appendices is 124 pages, which includes rich illustrative content of 29 figures (diagrams, schemes, screen shots) and 34 tables presenting data and classifications. The list of references contains 80 sources, demonstrating the breadth and depth of the literature review conducted.

III. CONTENT OF THE DISSERTATION

Introduction

The introduction clarifies the relevance of the problem and presents the methodological parameters of the dissertation, its structure, object, subject, goals and objectives.

CHAPTER 1 Standardized Information Security Management Systems

The first chapter of the dissertation aims to lay the theoretical foundations of the research. It provides a detailed review and analysis of existing approaches, standards and technologies in the field of information security management. The chapter is structured in such a way as to systematically identify the problems and gaps that the present work aims to address. A theoretical analysis has been made of the fundamental foundations on which the model of the Platform for Management and Automation of Standardized Information Security Management Systems is built, namely: Information Security; Information Security Standards; Information Security Management Systems (ISMS); and Software Applications for IS.

The chapter defines the terminology and aspects of information security, the methods, technologies and tools for information protection and the challenges that provoke the study. The evolution of information security from a purely technical aspect to a comprehensive management process is discussed. The need for a systematic approach to security management in organizations is presented, which goes beyond the framework of specific measures and ensures long-term sustainability.

Information security standards are analyzed, as well as the terminology, nature and objectives of standardization. The historical development of information security standards is examined, starting from early initiatives to the formation of international frameworks. The benefits of implementing standardized ISMS are discussed,

including improving management processes, reducing risk, increasing customer and partner trust, and complying with regulatory requirements. The main elements, architecture and processes for the development and implementation of an ISMS are examined. This section provides a detailed overview, describing the key elements of an IMS according to the standard, including:

- Organizational context - understanding internal and external issues, stakeholders and scope of the EMS;
- Leadership - senior management commitment, policies and allocation of roles and responsibilities;
- Planning - addressing risks and opportunities, security objectives and plans to achieve them;
- Support - resources, competence, awareness, communication and documented information;
- Operational activity - operational planning and control, information security risk assessment, information security risk processing;
- Performance evaluation - monitoring, measurement, analysis, evaluation, internal audit and management review;
- Improvement - nonconformities and corrective actions, and continuous improvement. Special attention is paid to Annex A of ISO/IEC 27001, which contains a list of security controls categorized by domain.

Despite the significant benefits, implementing and maintaining an ISMS is associated with a number of challenges. The difficulties that often lead to delays, increased costs or unsuccessful certification are analyzed. The following are discussed:

- Lack of resources - insufficient staff, budget and time;
- Complexity of processes - a large number of documents, procedures and control points;
- Resistance to change - difficulties in changing the culture and work habits in the organization;
- Documentation management - voluminous and dynamic documentation that requires constant updating;
- Audit and compliance - complex internal and external audit processes requiring comprehensive evidence of compliance;
- Continuous improvement - keeping the ISMS in constant compliance with changing threats and business needs.

These challenges serve as a basis for arguing for the need for automation and modeling to address these problems.

The first chapter also analyzes the market for software tools to support ISMS. The functionalities of leading products are studied and the following common shortcomings are identified:

- Passive documentation orientation - most systems are "electronic repositories" for storing policies, procedures, and records. They support auditing, but not active, dynamic management.
- Lack of semantic understanding - data is stored in relational databases that do not manage the complex semantic relationships between assets, threats, controls, and business processes. This limits the possibilities for automated analysis and inference.
- Poor process automation - processes such as risk assessment are often reduced to filling out spreadsheets that are then

uploaded to the system. There is a lack of true automation based on logical rules.

- Low flexibility and extensibility - systems are usually built around one specific standard and are difficult to adapt to other frameworks or organization-specific requirements.

Main conclusions of Chapter 1

- ☞ Based on the analysis of information security, information security standards and information security management systems, it is concluded that a comprehensive approach is needed to address the described progressive challenges.
- ☞ From the study of the types and functional scope of software applications related to ISMS, the segmentation of products is identified. ISMS comprehensive management systems are mainly in aspects of certification, re-certification and maintenance of the necessary records and templates for the purposes of the audit process. There is a lack of comprehensive solutions that manage and control all work processes and information flows in the infrastructure and superstructure of the organization. The platform approach to building an adaptive system that models and automates standardized information security management systems is an innovative, generalized solution to the treated issues.
- ☞ In order to ensure the efficiency, usefulness and reliability of the platform, it is necessary to develop a model that is based on comprehensive monitoring, analysis and management of the document matrix, workflows and information flows and assets of the organization.

CHAPTER 2. Modeling a platform for management and automation of standardized information security management systems.

Chapter Two presents a methodology for researching and modeling an automated standardized information security management platform, and in accordance with it, an analysis of the processes, determination of requirements, and identification of the general characteristics of the system are carried out. The research and analysis, according to the proposed methodology, includes the following key steps:

- **Process analysis**

Research and analysis of the standardized work processes that the system should automate and the corresponding information flows.

The following standardized work processes have been identified and described:

  - Implementation of business processes IBP/Document management ;
  - Platform administration processes;
  - Defining and managing business processes;
  - Management of SUS;
  - Monitoring and control;
  - Audit.

- **Determining requirements**

To determine the functional and non-functional requirements, the following was performed:

- Research and analysis of user groups;

Users of a platform for the management and automation of standardized information security management systems are divided into 2 large groups:

- Users - companies and organizations that have implemented an Information Security Management System certified to an internationally recognized standard. These are users from all sectors of the economy, operating in all sections of the classifier of economic activities, including state and municipal organizations.
- Certification and consulting organizations - perform audits for the certification of ISMS and control audits to confirm compliance.

- Research and analysis of information security standards;

The study of the requirements of the standards was carried out according to their main groups of characteristics:

- Content of the standard - name, purpose, policies, scope, requirements, conditions, definitions, type and area of applicability.
- Infrastructure - procedures, processes, documents, controls, registers, deadlines, tools and functional algorithms.
- Superstructure (external environment) - correspondents, customers, suppliers, partners and institutions, related standards, possible integration opportunities, audits, etc.

- Resources - organizational structure and personnel, assets, tools and materials needed to plan, maintain and control standard mechanisms.

  - Research and analysis of data.

A platform for the management and automation of standardized information security management systems, SUSI, operates with two main data groups, as follows:

- Data related to information security standards;
- Data related to the functional requirements for the Platform;

The result is shown in Appendix 3.

- **Defining the general characteristics of the platform**

The general characteristics of the platform were determined by studying good practices for user behavior, productivity, security and administration of information systems. Due to the specificity of the goals set and the subject matter studied, heuristic techniques were used for this task, such as:

- Best practices approach;
- Research and analysis of academic sources;
- SCAMPER technique;
- The Delphi Method

Unified Modeling Language – UML™ and Business Modeling – is used to describe the processes and requirements. Process Model and Notation (BPMN) standard for visual modeling of business processes in the form of diagrams like the ones shown below.

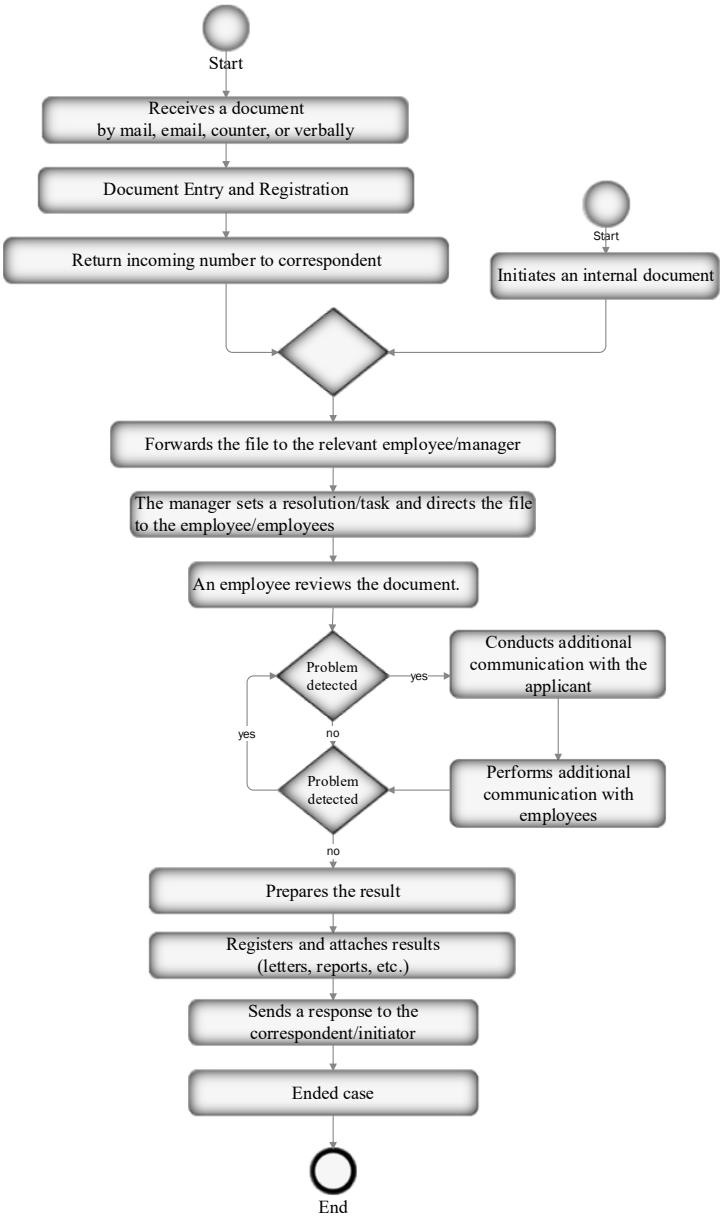

Figure 1Document Management Process

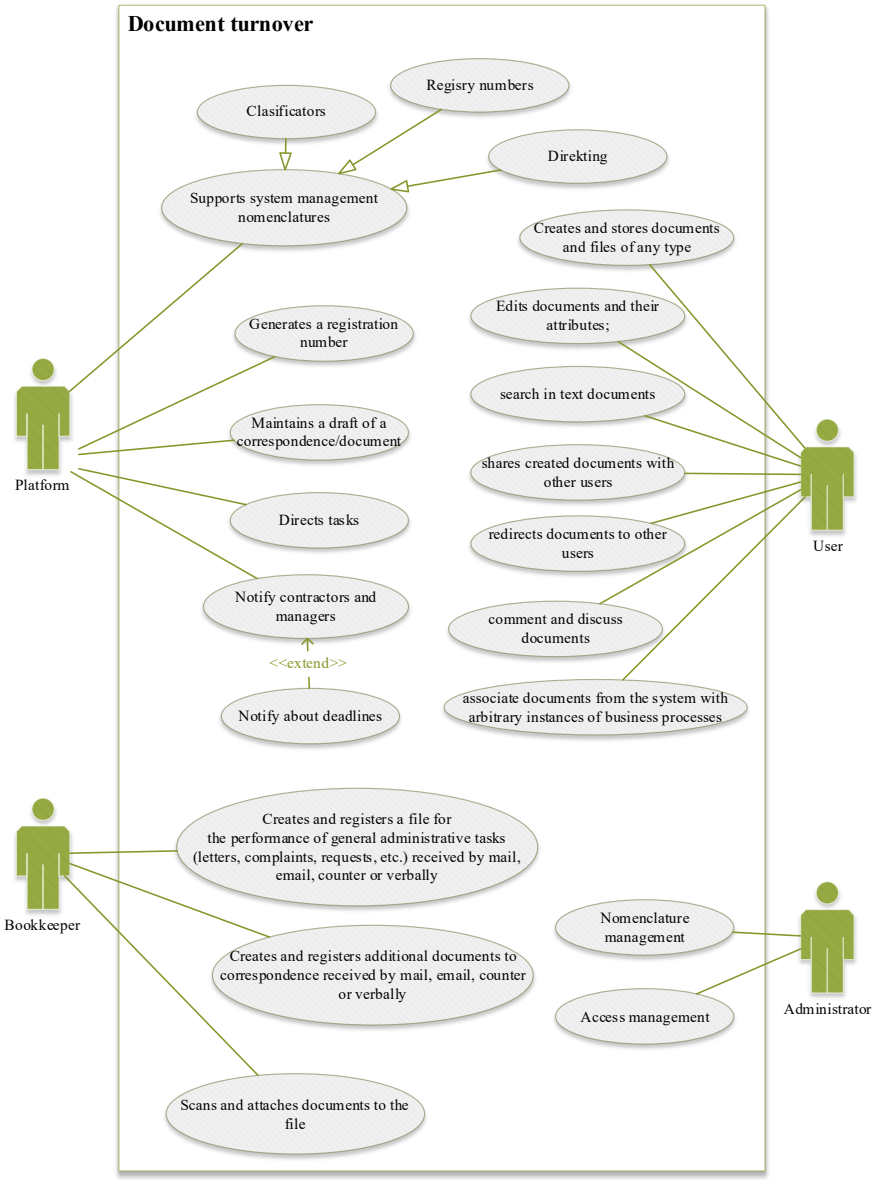

Figure 2Document flow diagram of user cases

Main results of Chapter 2

- An analysis of the standardized work processes to be included in the Platform model, subject to automation, and the relevant information flows corresponding to them, has been carried out.
- Based on an analysis of the data, user groups and information security standards, the functional and non-functional requirements that must be reflected in the modeling of the Platform have been determined.
- Good practices for user behavior, productivity, security and administration of information systems were studied and the common characteristics of the Platform were identified.
- The necessary input parameters, attributes and constraints for modeling the platform for management and automation of standardized information security management systems have been defined.

CHAPTER 3. Platform model for modeling and automation of standardized information security management systems.

In the third chapter, the author's theory of a document matrix is presented, as a basis for operational management of an organization and the company. The modeling methodology and the conceptual model of the Platform are described. An optimized model of the subject of the dissertation has been developed, built according to the theoretical foundations and the research and analyses presented in Chapter 1 and Chapter 2. A logical and physical architecture for the implementation of the platform is proposed.

Document matrix

Every company, regardless of its size, carries out its activities in an internal and external working environment. The internal environment is determined by the company's resources (human, material and intangible) and by the work processes within it, related to the subject of activity. The external environment is the customers, suppliers, partners and government institutions with which the company works.

Information security management systems according to internationally recognized standards define, regulate, manage, monitor, record and archive the internal and external operating environment through the organization's document system and the corresponding data sets.

A document is a record that reflects in its development every action, norm, event, resource, attitude, process and intellectual production. In addition to the fact that nowadays documents are electronic and paper, they can be conditionally classified into several formal groups - Conventional records and Specialized documents.

The quantity of all these records, called documents, define and determine the company, its history, capacity, quality and competitive ability.

Documents themselves are not independent separate units. They are connected in **a document network specific to each company.** Each document is a final product, behind which stands a process of varying complexity and scope. Each document process

consists of activities and stages and, as in any production, requires resources and materials. Resources and materials, in turn, are most often data sets and other documents that have their own processes and their own life cycle. The multitude of documents and the connections between them form the document network of the organization. Unlike the Internet, however, the document network of a company has defined paths, connections and forms (forms) and is connected to and indexes and manages the data sets (bases) of the organization.

For this reason, the system of company documents is considered not as the document network, **but as the document matrix** of the company.

The document matrix affects every element of the company's internal and external working environment and it is quite logical that it allows for maximum control over the organization. The company document matrix is the basis of the management of any management system built according to internationally recognized standards. They are based on policies, work processes, procedures and numerous forms and records for their control.

When documents are digitized, the connections between them are visualized, and the matrix is dressed in appropriate functionality, an extremely effective system for monitoring, controlling, and managing all levels and resources in the company is obtained.

Platform concept

The platform for modeling and automation of standardized information security management systems is a modern, innovative, integrated information and operational system that models, digitizes, registers, manages, stores and controls work processes and related information and documentation in accordance with various internationally recognized information security standards.

The model is based on monitoring, analysis and management of the document matrix, workflows and information flows and assets of the organization. The platform covers all information units - documents (paper and electronic), audio and video communications, system, program and communication logs, etc. It monitors incoming, outgoing and internal information flows and manages them according to the workflows and standardized forms modeled in it.

Workflows and standardized forms are modeled according to the policies, procedures and templates of the information security management systems (ISMS). All records related not only to the elements of the ISMS, but also to the operational processes are formalized in the platform and are carried out only through it. The goal is to use the latest technological advances to digitize, index and revitalize the document matrix of the organization and enable operational efficiency of security management.

Information assets are introduced into the Platform as parameterized objects. Each control from the system of controls of the information security standards, according to which the ISMS is built, is associated with one or several predefined criteria of the platform. Each criterion is a formalized record with certain

parameters of the registered information and frequency and method of verification. For each criterion, triggers for platform action are defined, according to possible values or events.

Controls are applied to an asset and/or process in accordance with the ISMS.

The mission of the platform is to integrate all document flows related to the work processes in the client organization. To connect the many application software products working in the field of information security and data arrays into a single information, communication and management system. The platform unites information sections and information flows into a single information space and provides an integrated environment for storage, management and exchange. This allows to effectively monitor the movement of information structured into separate types of document units, to model the IMS and to implement reliable control.

The platform models the hierarchical structure of the organization, with the possibility of changes, allowing for adequate distribution of tasks according to the company's subordination. The system manages the movement of various types of documents, automating all phases of workflows.

According to the research and analysis presented in Chapter 2, the platform for modeling and automation of standardized information security management systems is implemented with the following components (modules):

- Module for defining and managing business processes DBP;
- Business Process Execution Module IBP;
- ISMS module;
- Audit and Control Module;
- The administrative module;

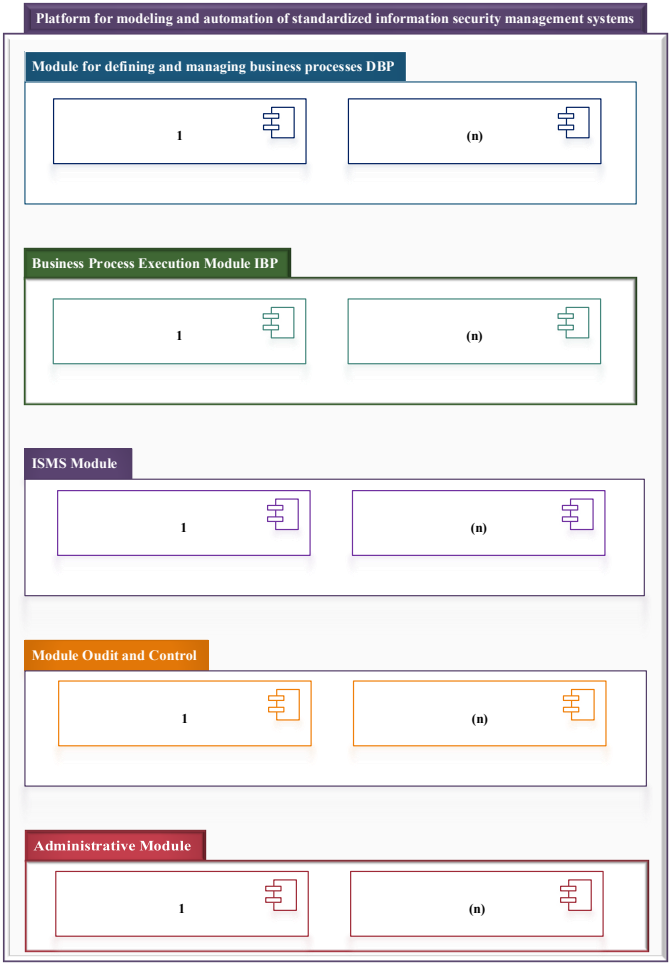

Figure 3Platform Structure

The platform uses a single database in which the necessary information is entered and output through various interfaces, according to the information classes. The base arrays are managed by building specialized logic for each of them - standards, terms, processes, users, procedures, routes, forms, controlled processes, and various unstructured data. The platform layer, the so-called middleware, implements the logic and exchange of information between the interfaces for entering information and the database. Another platform layer implements the connection of the functional modules and the database. The functional modules (components) perform a certain group of functions by providing interfaces for performing the necessary tasks. The platform builds its modules in the context of each client organization, as a set of components (functional modules) as shown in the figure.

The system has a registration and control part, in which the organization's indexes are entered and all incoming-outgoing and internal operational documents (events) are registered in accordance with them. Document numbers are automatically generated according to a pre-set stereotype. Deadlines for execution can be set for each registered document, which it controls. The platform also functions as a communicator, informing in various ways (e-mail, SMS, sound and visual) about various controlled events, overdue deadlines and tasks to be performed. The electronic system models the operational procedures and process maps created in the company according to the relevant standard, ensuring the informationally correct compliance with all work processes, filling in the relevant forms and blanks, monitoring of work processes and control of

decisions. It guarantees the highest possible levels of security, reliability and information protection. It provides the opportunity for each user to identify themselves not only with a username and password, but also with a private electronic signature. Each employee/user has pre-defined profiles, roles, access rights and functionality corresponding to their job description. The system dynamically generates personalized screens upon user login, providing an intuitive user interface and navigation.

The modules of the Platform build the models related to the management of various types of internationally recognized standards with a rich set of tools: **standardized processes; pre-developed scenarios and stagings;** a set of predefined forms; developed conventional registers; specialized registers; internal communication environment; systems for evaluation, control and audit support; and others.

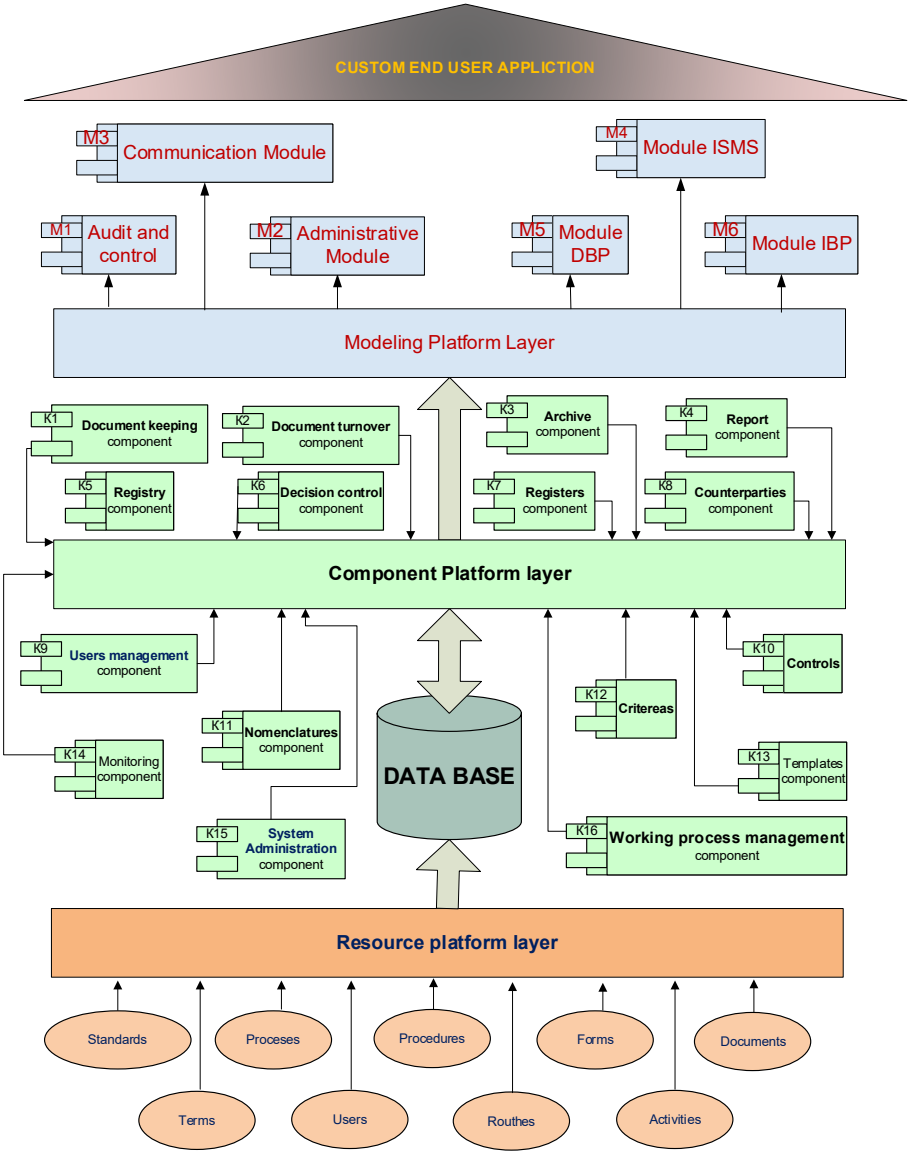

Figure 4Conceptual architecture of the model

Modeling methodology

Based on functional and non-functional requirements, business processes and the specification of user cases defined in the previous chapter, after the research and analysis, an optimal set of information descriptors was developed, distributed into logical information classes and subclasses.

The set of descriptors generated by the research and analysis is decomposed into logical information classes, in accordance with their functional orientation in the description of the standards. Information classes are considered as program objects and sub-objects. They are described by their attributes, which are called information identifiers. Their representation is unified by using a specific technical format that defines the format of representation of the values of each attribute of the information objects. The technical format of the information classes and their attributes is described by the syntax of the Unified Modeling Language (UML).

For the design of the platform, UML class diagrams are used. which depict the structure of the system by modeling its classes, properties, operations and relationships between objects. A class diagram is a visual notation used to build and visualize object-oriented systems. It is a static structural diagram demonstrating the properties of the platform, classes, operations and relationships between objects for the description and design of the system. Class diagrams are a form of structural diagrams, as they determine what should be included in the modeled system. Information identifiers are modeled in 3 levels of information classes structured in modules

of the platform. As an example, I apply a model of one main SUSI module.

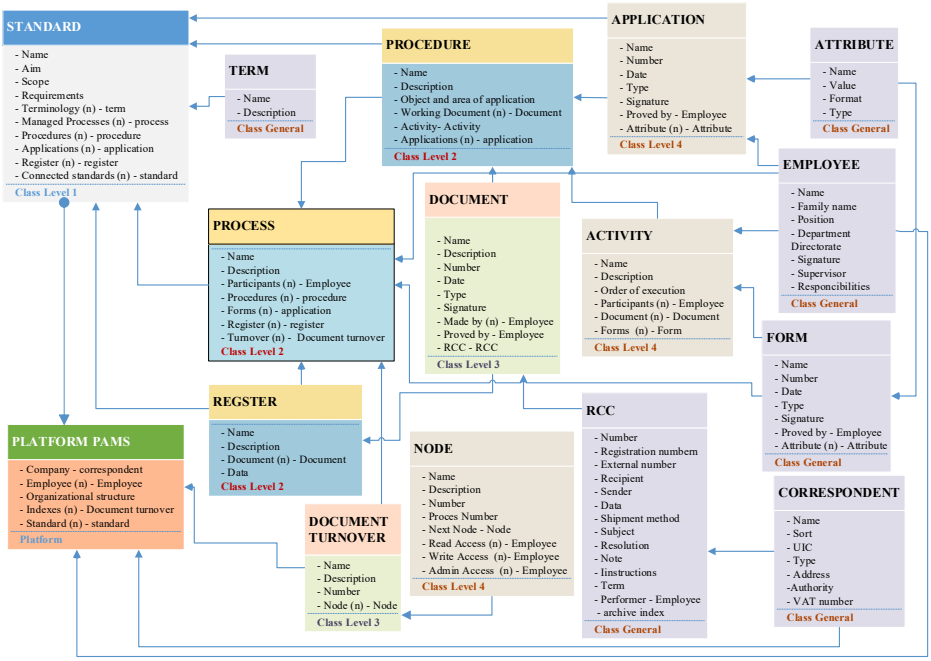

Figure 5 SUSI module

The identifiers for each class are described in detail in a tabular form.

Table 1Organizational Unit (Structure)

Description		
Type	**Name/ Format**	**Description**
Class	Organizational unit: () Structure	Organizational Unit (Structure) is a base class of the Administrative Module, related to describing the structure of the organization and its corresponding modeling in the Platform.
Attribute	Name: Nvarchar (400)	Name of the organizational structural unit.
Attribute	Type: Type	The structure type is a predefined nomenclature – directorate, department, sector and position.
class	Parent Organizational Unit: Structure	Name of the parent organizational unit to which the structure belongs (if any)
Subclass	Rights (n): Right	A list of rights on the information objects that the organizational unit and all its substructures have. A set of rights are defined for each information object from the classifier - Example: for the information object "Incident Register" the right to read, the right to register and the right to edit.
Type	**Name/**	**Description**

	Format	
Subclass	Templates: Template	Templates are a set of rights that can be applied to any information object and added as a structural unit in a set.
Subclass	Users: User (n)	A list of employees of the organization who have been added to the organizational structure.

System architecture

The platform for modeling and automation of standardized information security management systems is implemented as a centralized web-based system with a service-oriented architecture (SOA), combining the main modules, which in turn use an infrastructure of standardized services to implement processing for specific types of information.

Service-oriented architecture (Service- oriented Architecture) is a model specifically designed to reduce costs, increase flexibility and simplify the presentation of business and operations of different parts of the activity. A basic principle of SOA is the structuring of business activities into services, which allows for their rapid identification and reuse of already existing functionalities, as well as avoiding their duplication during development. Standardization of the behavior of these services leads to limiting the unexpected impacts of changes, as well as to their successful prediction and avoidance. Service-oriented architecture (SOA) is a collection of independent software elements that provide software functionality to other applications as a service.

Main advantages of the SOA approach:

- Independence from supplier, product or technology;
- The service is a self-contained functional unit.

The Services can be combined with other software applications to provide full functionality of a larger software application.

Logical architecture

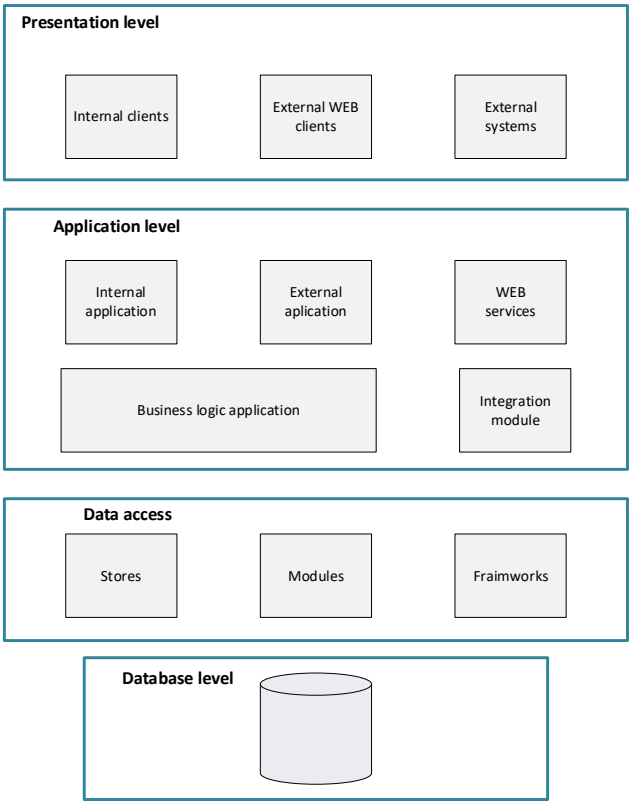

Figure 6 System architecture of the Platform implementation – three-tier MVC architecture

The platform architecture can be decomposed into separate layers (levels), communicating with each other via strictly defined interfaces. The main advantage of this approach is that it allows significant changes to be made to individual layers without affecting the others, which leads to extreme flexibility. The layers are defined to group elements that vary independently. In centralized platforms, a proven model is the separation of the following layers:

- Database layer;
- Business logic layer;
- User interface layer (presentation layer);

Each layer is subsequently decomposed into separate modules, with communication between the modules being carried out via strictly specified interfaces. The division into clearly defined layers and the separation of the database layer from the business logic layers allows for the overall solution to be compatible with both the existing infrastructure in the organization and with a virtual infrastructure.

Physical architecture

The platform is based on a flexible architecture that can be deployed in both a physical environment and a virtualized (cloud) environment, or another hybrid solution.

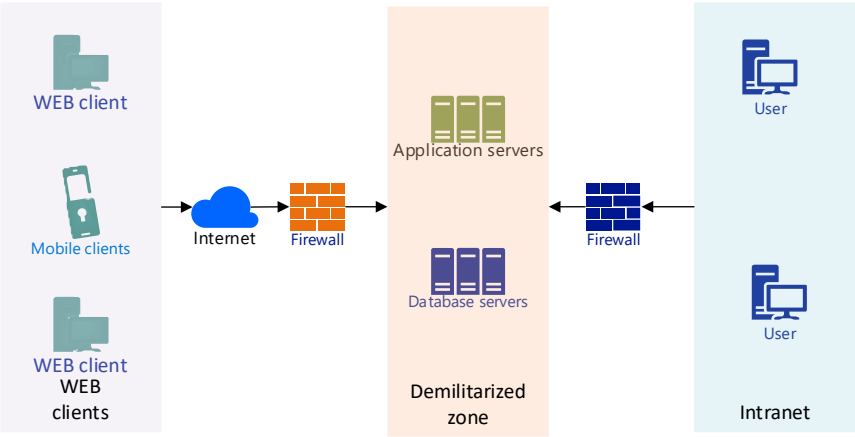

Figure 7Physical architecture

The platform adapts to the organization's existing hardware, network and application environment, and has two main physical components:

- An application server that executes requests to the system's web application through which users work with the system.
- Server for managing the system's databases.

Considerations for maximum separation and ensuring information security predetermine the separation of servers in the so-called DMZ or "demilitarized zone" - an area of the network that is isolated from the rest of the internal network, separated from the external environment by an external firewall, but also by an internal firewall, so that a possible breach does not pose a risk to the server with the system application or the server storing its databases.

Main conclusions to Chapter 3

- **The Document Matrix** is introduced as a basis for operational management of the company and the conceptual model of the Platform.
- According to the described modeling methodology and the results of the previous chapters, a model of the Platform for Modeling and Automation of Standardized Information Security Management Systems has been built.
- A logical and physical architecture for the implementation of the platform is proposed.
- The UML code of the model is presented in **Appendix 5 (Plant UML)**
- The implementation of the Platform in modules with Python in OOP style is presented **in Appendix 6.**
- The database implementation is given in **Appendix 7** ORM (Object-Relational Mapping) implementation via (SQL Alchemy standard in Python).

IV. MAIN FINDINGS AND CONCLUSIONS

Scientific contributions

- An algorithm and methodology for research and modeling of an automated standardized information security management platform are proposed;
- The author's theory of **a document matrix is presented** as a basis for operational management of an organization and a company.

Scientific and applied contributions

- An analysis of information security management systems is presented in aspects: Information security; Information security standards; Information security management systems (ISMS); IS software applications.
- Work processes and flows that are subject to automation through the developed platform have been identified, defined and analyzed;
- Functional and non-functional requirements are defined after research and analysis of data, user groups and information security standards;
- The general characteristics of the system are identified, using heuristic methods;
- A model of a complex platform for modeling and automation of standardized information security management systems has been developed. The model is based on monitoring, analysis and management of the

document matrix, workflows and information flows and assets of the organization.

- A platform architecture is proposed that is in line with modern requirements for modularity, automation, and standards compatibility.

Directions for future research

The results achieved in the dissertation work outline the following directions for future research:

- Development of the Platform with integration with artificial intelligence that analyzes:
  - Information units and records;
  - System, program and communication logs;
  - The information generated by the control criteria.
- Based on the analyses performed with AI, the platform's functionalities can be further developed in aspects:
  - Offering optimization of the SUS;
  - Display of abnormal parameters and activities outside the norm;
  - Calculating probabilistic events and predicting risk factors.
- Information security management systems can be modeled with neural networks managed by the Platform. This is an approach to increasing the effectiveness and efficiency of critical information security management systems.
- The generative unsupervised neural network - Boltzmann machine (Boltzmann Machine) uses techniques on input data to analyze the normal states of the IMS to predict undesirable

situations. Internationally recognized standards define a set of security controls for monitoring, auditing, and managing the IMS. They are divided into categories, and each of them has standardized attributes. The neural units of the Boltzmann machine are based on the IMS security control infrastructure.

- Integrating neural networks into an ISMS can significantly improve an organization's ability to detect, predict, and respond to security anomalies. NNs are widely used in almost all areas of information and cybersecurity, but for modeling the behavior of an ISMS as a complete complex system, they are an innovative method for reducing costs and time, as well as preventing or mitigating damage.

Approbation of the results

The main results obtained in the development of the dissertation work have been reported in three publications and at specialized international conferences.

Articles and citations

1. Velev T., Dobrinkova N., “Unified innovative Platform for administration and automated management of internationally recognized standards”, Book Title: “Digital Transformation, Cyber Security and Resilience of Modern Societies”, book series “Studies in Big Data", Springer. DOI:10.1007/978-3-030-65722-2 _5, eBook ISBN: 978-3-030-65722-2, ISBN: 978-3-030-65721-5, (https:// www.scopus.com /pages/publications/85129091048) ISSN: 2197-6503, vol. 84, p. 75
2. Velev T, "Heuristic essentials for modeling and optimization of a platform for automation and management of standardized information security management systems" , 28–29 October 2021,

Sofia , Bulgaria , 2021 Big Data, Knowledge and Control Systems, Engineering (BdKCSE) IEEE | DOI: 10.1109/BDKCSE53180.2021.9627263 , ISBN:978-1-6654-1042-7, https:// ieeexplore.ieee.org /document/9627277 ;

3. Velev T., Dobrinkova N., "The logical model of unify, innovative Platform for Automation and Management of Standards (PAMS)" 1st International Scientific Conference Digital Transformation, Cyber Security and Resilience " DIGILIENCE2019, Sofia 2-4 October 2019. ISIJ Digital Transformation, Cyber Security and Resilience, ISSN 0861-5160 (print), ISSN 1314-2119 (online), vol. 43, no. 1 (2019): 113-120, 2019, p.113-p.120 https://doi.org/10.11610/isij.4310
   - Citation 1: Wang, Z., Guan, X., Zeng, Y., Liang, X. and Dong, S., "Utilizing data platform management to implement "5W" analysis framework for preventing and controlling corruption in grassroots government". Heliyon Volume 10, Issue 7, 15 April 2024, e28601, DOI: 10.1016/j.heliyon.2024.e28601, 2024 (Scopus referenced: https: // www.scopus.com/pages/publications/85188751354)

Conferences

- International Conference on Big Data, Knowledge and Control Systems Engineering BdKCSE'2018, (21-22 November 2018), report: "Unified innovative Platform for administration and automated management of internationally recognized standards"
- DIGILIENCE 2019: Digital Transformation, Cyber Security and Resilience Central Military Club Sofia, Bulgaria, October 2-4, 2019, report: " The logical model of unify, innovative Platform for Automation and Management of Standards (PAMS)"

Projects

Part of the research in the dissertation is from project No. BG161PO003-1.1.06–0036-C0001 “Unified platform for administration, automation and management of internationally recognized standards”, implemented in cooperation by the teams of **Perfect Plus EOOD (head Todor Velev) and IICT - BAS (head Svetozar Marg e nov).** The project is for industrial research of a high-tech innovative product in the field of information technologies with a duration of 22 months.

A large part of the results has been tested in the project "Development and implementation of a Unified System for Management, Control and Analysis of Activities (ESUKAD) for the needs of the Bulgarian Institute of Metrology (BIM)", led by Todor Velev.

Acknowledgements

I express my gratitude to my supervisor, Prof. Dr. Nina Dobrinkova, for valuable guidance, professional competence and assistance in the preparation of the dissertation. I am grateful for the help and advice of my colleagues from the Institute of Computer Science and Technology of the Bulgarian Academy of Sciences and from Solent. University of Southampton.

Applications

Appendix 1 Basic terminology in standardization
Appendix 2 Certification (auditing) organizations
Appendix 3 Data Exploration
Appendix 4 Up-to-dateness and change of documents and records management.
Appendix 5 UML model code (Plant UML)
Appendix 6 Platform implementation with Python
Appendix 7 ORM (Object-Relational Mapping) implementation – SQL Alchemy

Content