Assessing the level of security of enterprise information systems

Tetiana Babenko[1,2,†], Hryhorii Hnatiienko[1,†] , Larysa Myrutenko[1,†], Andrii Bigdan[1,3,†] and Viktoriia Hrechko[1,†]

[1] *Taras Shevchenko National University of Kyiv, 64/13 Volodymyrska Street, Kyiv, 01601, Ukraine*
[2] *International Information Technology University, 34/1 Manas St., Almaty, 050000, Kazakhstan*
[3] *Blekinge Tekniska Högskola, 371 79 Karlskrona, Sweden*

Abstract

This study presents the development and implementation of an intelligent model for assessing the level of maturity of information security processes for enterprise management systems and justifies the universality for organizations of various types. The objective of the developed model is to comprehensively support information security specialists and auditors in assessing the levels of maturity of information security processes of management systems. The model was developed using a feedforward neural network based on the ISO 27000 / NIST 800 family of standards security controls. The model allows an accuracy of 96-99% to assess the level of maturity of information security processes in the enterprise. The methodology described in the document can be extended to enterprises with different functions and different forms of ownership. The possibility of assessing the level of security (implementation of controls) based on assessing the maturity of information security processes is investigated. The article evaluates and justifies the universality of the proposed solutions based on the maturity assessment of information security processes built based on 800 standards. The developed model can be used as part of a decision support system to help specialists identify the strengths and weaknesses of existing information security management processes, choose risk treatment approaches to ensure business continuity in a hostile cyber environment, improve the information security management system, which will affect the use of enterprise resources.

Keywords information security, security assessment, maturity model, neural network, risk management, decision support system, information security management system, countermeasures, assessing the security of information systems, network security

1. Introduction

The activity of any enterprise is aimed primarily at meeting the needs of stakeholders. Main business processes are focused on achieving this goal. Therefore, the management of the enterprise is interested in that the processes within the organization were under control, and functioned as intended, and the number of threats and errors was minimal. Otherwise, successful threat execution can lead to data leaks, damage, or unauthorized modification of the information that causes financial and reputational losses. By threats, we mean a potential threat to information or a system [1]. The main definitions are Risk, Asset, Event, Countermeasures, Reputation, and Regulatory fines. Risk is the probability that a source of threat will exploit a vulnerability, leading to a negative impact on the business [1]. Risk can be calculated as the product of the emergence of a threat (event expectation/ year) and loss in a defined currency. Companies implement countermeasures to provide the appropriate level of asset security (Figure 1). Regulatory fines – this type of damage can occur when, for instance, a hospital does not comply with the Federal Health Insurance Tolerance and Accountability Act (HIPAA) [2] and the confidentiality of patient information decreases.

DTESI 2024: 9th International Conference on Digital Technologies in Education, Science and Industry, October 16–17, 2024, Almaty, Kazakhstan
* Corresponding author.
† These authors contributed equally.
babenko.tetiana.v@gmail.com (T. Babenko); g.gna5@ukr.net (H. Hnatiienko); myrutenko.lara@gmail.com (L. Myrutenko)
0000-0002-5190-4742 (T. Babenko); 0000-0003-1184-9483 (H. Hnatiienko); 0000-0002-0465-5018 (L. Myrutenko)

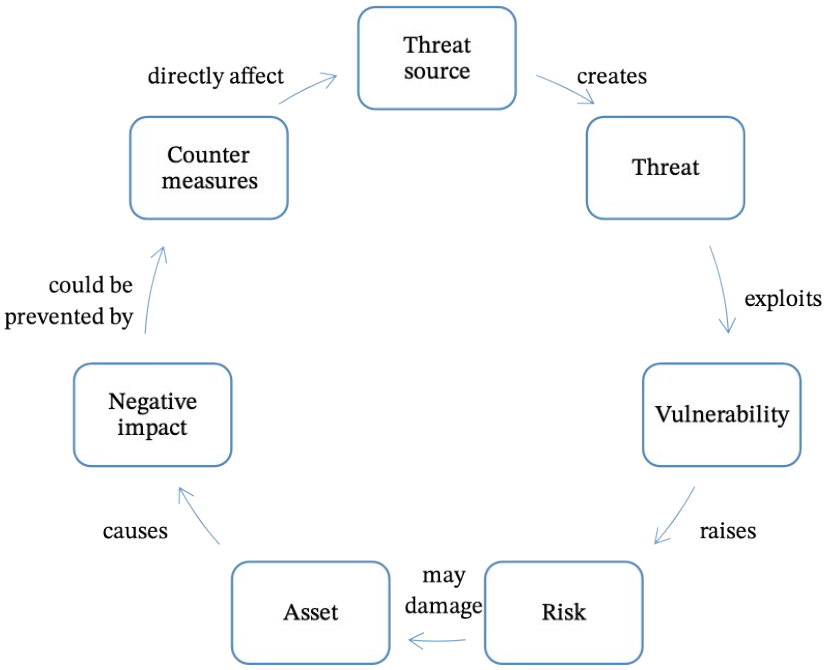

Figure 1: The risk-based approach to building an information security management system.

Various types of countermeasures have their own goals. Some of them intend to restrict physical access. They include password access systems, retinal or fingerprint scans, and security guards [3]:

- password access systems;
- scanning of the retina or fingerprints;
- security, etc.

Others set to block access and/or maintain data confidentiality across the organization networks:

- firewalls;
- means of data encryption;
- antiviruses and spyware scanners.

In addition, some countermeasures have been developed to quickly restore in the event of a successful intrusion, such as backup. To improve the efficiency of operational and strategic management of the development of information systems, a specialized analytical apparatus is needed for making managerial decisions [4]. A feature of the subject area of this problem is the complexity of its formalization, the presence of uncertainties associated with the incompleteness of data, the periodicity, and seasonality of the processes under study, the presence of a significant number of interconnected, not only quantitative but also qualitative indicators that characterize them [5]. A maturity model is a tool for assessing the effectiveness of implementing business processes in an organization and allows management to effectively track progress [6], and determine their strengths and weaknesses. Typically, an information security maturity model describes a set of characteristics that include the following features [6]:

- effective leadership and management,
- information security risk management processes,
- used a set of technologies.

Thus, to provide information resources, it is also necessary to develop information security management systems (ISMS). Since the objects of management are rather complex organizational

and technical structures that operate under conditions of uncertainty, for the effective management of such systems, it is advisable to use information decision support systems (DSS) based on intelligent information technologies.

The object of the study is the process of classifying the level of security maturity of information systems using a model synthesized based on neural networks using the backpropagation learning method.

The study aims to develop a model for classifying security process maturity levels and to present a software tool for conducting the audit process.

As part of this study, the following steps are to be carried out:

1. The accumulation of input data is a collection of elements that describe the characteristics of the available security-related processes.
2. We are obtaining and processing data to perform simulations.
3. Synthesis of a neural network.
4. Neural network training.
5. Assessment of the adequacy of the synthesized model.

2. Literature review

An overview of the maturity models of information security management processes or processes in various areas [7]. A review article by Portuguese authors D. Proença, J. Borbinh [8] collected and analyzed the current practice of maturity models.

A study by Faith-Michael E. Uzoka [9] shows that 77% of organizations (using the example of Botswana) spend heavily on the development of their IT services, but some of them remain at a low level according to the CMM. The staged CMM structure that was used in this study is based on the principles of product quality supported by Schuart and Deming (1939). Organizations find this model costly and prefer to invest in other businesses. Despite not using the CMM, many organizations have reached a high level of maturity. A significant 49.4% of organizations have reached maturity level 5, and 7.4% are at maturity level 4. The results show that a total of 56.8% of organizations are at higher maturity levels. Reasons for low maturity include [9]:

- low level of training and qualification of employees,
- poor working conditions and incentives for employees,
- poor documentation of software and architecture requirements, integration of software components,
- low use of appropriate technology,
- low management culture, etc.

An article by Chinese researchers Wei Han, Xiu-Yan Sun et al. [10] explores methods for using data in the field of network security. The authors have classified semantic relationships between network security resource classes, subclasses, and different data types. As a result, better network data security was created due to a single standard for the transmission of an information resource, and a data exchange platform was developed that applies the above metadata standards.

A joint article by Chinese and American researchers Wangshu Li, Wenhao Yan, et al. [11] considers the mathematical apparatus used to protect the information in information systems. In particular, a discrete method for a continuous chaotic system is introduced and the Euler stability principle for a discrete system is obtained. The authors have developed three methods for realizing the synchronization of a discrete chaotic system.

The ISO/IEC 27001 standard aims to create an information security management system in a company [12]. For example, in the ISO 27001:2013 standard, there are requirements for the existence of a risk analysis procedure in an organization. The question always arises: how to meet these requirements, to what extent, and at what level of detail for companies of different sizes. Very often

information security managers pay attention to the size of the organization and rarely to the level of its organizational and technological development.

The answer to this question will help to give a maturity model based on an assessment of the level of maturity of the information security processes of enterprises [13].

The process of collecting data from different sources, and pre-processing for use in an analytical model, is described in [5,14,15]. At the end of this process, a numerical dataset is obtained, which will become the basis for training, testing, and evaluating the model. The data collection process for assessing the maturity of an information system and a questionnaire prepared to take into account 11 areas of the ISO/IEC 27001 standard are given in the work of V. Hrechko, T. Babenko, and H. Hnatiienko [16]. However, there are no open datasets for assessing the maturity of information systems. The reason for this is the confidentiality and ethics of corporate data.

3. Materials and methods

3.1. The structure of the information security maturity assessment model for enterprise management systems

Figure 2 shows the structure of the developed model. The input information is the assessment data of security controls of international standards ISO/IEC 27002:2013/NIST 800, information on the level of implementation of the relevant security controls at a particular enterprise (in the range 0..5). This information is used to form an array of initial data in digital format represented by the vector E (0..m). Based on the ratings, a data status vector is formed, which contains its rating (from the set of attribute A) for each of the security measures (which can be from 1 to 700). This is followed by the stage of pre-processing and preparation of data for training the model. This table is fed to the input of the neural network, and as a result, at the output we get the level of maturity of the information security management system in the form of a single number, also from the attribute set A (that is, in the range 0..5). As an element of the decision support system, the model also provides feedback, which allows how to process information security risks.

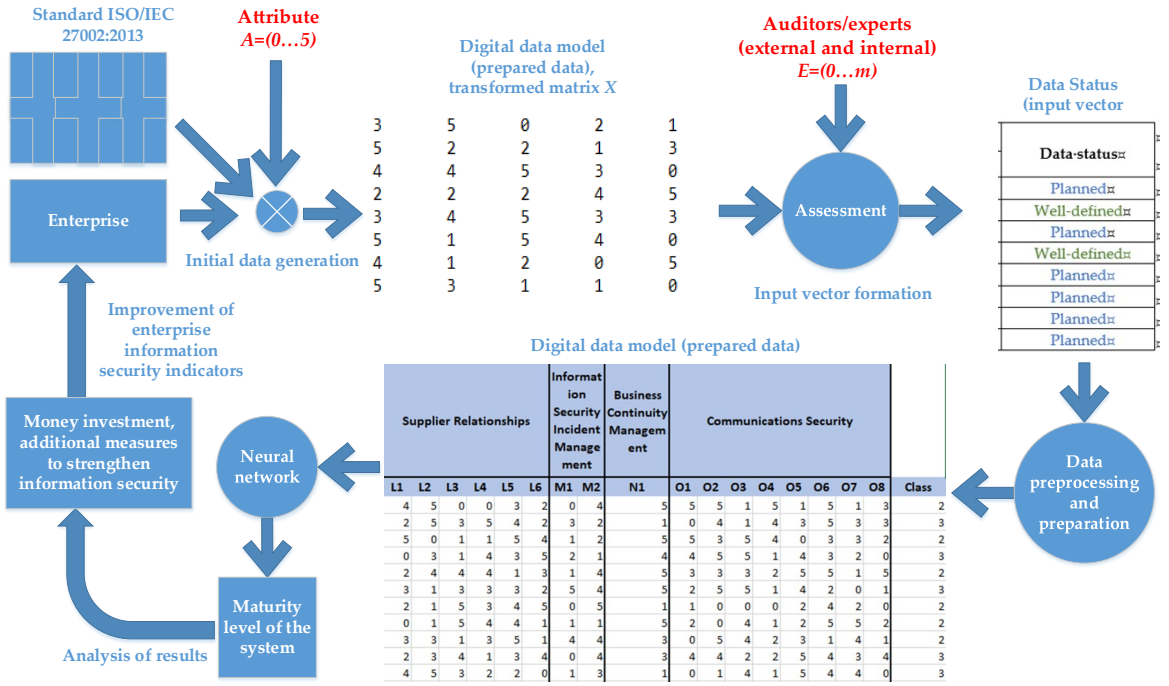

Figure 2: Structural diagram of the model for assessing the maturity of information security management processes for enterprise management systems.

The maturity model can be considered as a structured set of elements detailing the features of effective ISMS processes, then the number of nodes at the input level is equal to the number of ISO/IEC 27002:2013 controls, and the input data for each node is the calculated value for specific security control, respectively [14].

Thus, the input vector can be defined as in (1):

$$X^T = [x_1 x_2 \cdots x_n], x_i \in I = \{0, \ldots, 5\}, \quad (1)$$

where $x_1, x_2, \cdots, x_n$ denote the score for ith security control and n is the number of nodes in the input layer.

The output layer of the model consists of 6 nodes representing the level of maturity of information security management processes, as described earlier [14]. The number of neurons in the hidden layer is determined according to best practices since the arithmetic means between the number of nodes in the input and output layers is 60.

3.2. Using maturity models in assessing the security level of information systems

To determine the stage of organizational and technological development of the organization the concept of the maturity model was created [16]. There are many maturity models across different fields, including cybersecurity. Global practice shows that often those models are developed by government agencies for specified tasks to achieve national or international standard status. The Cybersecurity Capability Maturity Model enables organizations to evaluate the current level of capability of their practices, processes, and methods and prioritize actions and investments to improve cybersecurity [17]. The base of the Capability Maturity Model is a process-oriented approach. One of the first models of this type was the Maturity Model designed by the Software Engineering Institute (SEI) in the mid-1980th. An overview of information system maturity models, including their origin, is given in [18].

Information security capability maturity models are broadly classified as follows:

- Fields: how are general concepts of organizational processes connected?
- Goals and measures: goals mean the desired values of indicators that should be acquired in each of the model areas, and indicators help visualize progress toward achieving goals.
- Maturity levels: it is the result of assessing the implementation of goals and measuring indicators in the areas of the organization.

The value of maturity ranges from the initial level, when the organization may have just begun to consider cybersecurity, to a dynamic comparison, when the organization can adapt quickly to changes in cybersecurity on threats, vulnerabilities, risks, economic strategy, or change needs.

The value of maturity ranges from entry-level, when an organization may have just begun to think about information security, to dynamic comparison, when an organization can quickly adapt to changes in information security in terms of threats, vulnerabilities, risks, economic strategy, or changing needs. As a result of a literature review on the topic, the most popular (based on the citation index of publications on this topic according to the Scopus scientometric database) maturity models were identified: SSE-CMM (System Security Maturity Model – Capability Maturity Model) [19,20], C2M2 (Cybersecurity Capabilities Maturity Model) [17,20], CCSMM (Community Cyber Security Maturity Model) [17,21], and NICE (National Initiative for Cyber Security Education – Capability Maturity Model) [21]. A comparative analysis of maturity models in the field of information security is given in Table 1.

Table 1
Comparative analysis of maturity models in the field of information security

Feature	C2M2	NICE	CCSMM	SSE-CMM
Focus on cyber security	+	+	+	–
Year of last revision	2014	2014	2006	2008
Security frameworks compliance	NIST	–	NIST	–
Risk management level	Detailed	General	General	Detailed
Industry	Energy	Production	Public associations	Security engineering
Defining roles and responsibilities	+	+	–	+

There are significant similarities between information security capability maturity models. The main difference lies in the area they target and the level of best practices that should be applied. C2M2 is the only mature, cybersecurity-centric information security capability model that is updated and focused on the entire organization. All information security capability maturity models are based on information security risk management, but only SSE-CMM and C2M2 measure risk management in a more specific way.

Other information security capability maturity models include ISM3 [5,22] and COBIT [22,23] (Table 2). ISM3 is a model that manages information security metrics that help an organization maintain an acceptable level of risk, even if tailored to specific needs. The model focuses on information security rather than cybersecurity. The last three versions of COBIT (since 2005) focus on IT leadership and governance. Similarly, models not used in the studies or not mentioned were included.

Table 2
Evaluation of the scope of ISO/IEC 27001:2017 security controls

Maturity model	A1	A2	A3	A4	Sum
Open Information Security Management Maturity Model (O-ISM3)	2	3	4	4	13
Systems Security Engineering – Capability Maturity Model (SSE-CMM)	2	4	4	2	12
ISF Maturity Model Accelerator (ISF MM)	2	2	3	3	10
Control Objectives for Information and Related Technologies - Version 2019 (COBIT 2019)	4	2	4	2	12
Oil and Natural Gas Subsector Cybersecurity Capability Maturity Model (ONG-C2M2)	3	2	2	3	10
Building Security in Maturity Model (BSIMM)	3	4	4	4	15
Average score	2.6	2.8	3.5	3.0	12

A new maturity model should be developed if no existing model can solve the identified problem. The developed maturity model of ISMS presented in Table 3 adopts the established structural elements, scopes, and functions of the best practices found in ISO/IEC 27001. An iterative process (in general, two iterations) was established for the evolvement of the specified maturity model, the design process of the model is shown below.

In the first iteration, the characteristics and structure of the maturity model were determined. Five levels of maturity have been proposed: initial, managed, defined, quantitatively managed, and optimized. The first iteration focused on only the planning phase of the ISO/IEC 27001 ISMS process.

For each criterion of the maturity model, it was simulated how this criterion manifested itself at different levels of maturity.

Table 3
The maturity model of ISMS

Maturity level		Controls
Level 1: Planning	2.1	Definition of scope and limits of ISMS
	2.2	Development of ISMS policy
	2.3	Approach definition for risk assessment
	2.4	Risk identification
	2.5	Risk analysis and risk assessment
	2.6	Determination of risk treatment options
	2.7	Determination of objectives and control criteria for risk treatment
	2.8	Obtaining permission to approve residual risks
	2.9	Obtaining permission to implement and operate ISMS
	2.10	Preparation of an applicability provision
Level 2: Implementing	3.1	Drawing up a risk treatment plan
	3.2	Implementation of a risk treatment plan
	3.3	Implementation of selected control.
	3.4	Defining measures of the implemented controls' effectiveness
	3.5	Implementation of training and awareness programs
	3.6	Management of ISMS operation
	3.7	Management of ISMS resources
	3.8	Implementation of procedures and other controls to promptly identify security events and respond to security incidents
Level 3: Monitoring	4.1	Monitoring and reviewing procedures and other controls
	4.2	Conduction of regular reviews of ISMS effectiveness
	4.3	Measuring the effectiveness of controls
	4.4	Reviewing the risk assessment
	4.5	Reviewing the residual risks
	4.6	Reviewing the identified acceptable risk levels
	4.7	Conduction of regular internal audits
	4.8	Reviewing ISMS
	4.9	Updating security plans
	4.10	Logging actions and events
Level 4: Improving	5.1	Implementation of defined improvements in ISMS
	5.2	Taking appropriate remedial and preventive actions
	5.3	Informing all interested parties about actions and improvements in ISMS
	5.4	Ensuring that improvements achieve their intended objectives

In the second iteration, the definition of maturity levels was completely revised, proposing five new levels of maturity: initial, planning, implementing, monitoring, and improving. These maturity levels are based on the PDCA (Plan/Do/Check/Act) cycle used in ISO/IEC 27001. Table 3 describes the controls on which the proposed maturity model is based. It makes it easier for users familiar with ISO/IEC 27001 to understand this maturity model and trace the relationship between what is required in each assessment criterion and the requirements specified in ISO/IEC 27001.

Model tuning is usually superimposed on the model training phase. Some parameters determine how the model performs at a high level (learning function or modality) and cannot be learned from the input. These hyperparameters must be tuned manually, but sometimes they can be tuned automatically by searching the model parameter space – hyperparametric optimization [24]. It is often performed using classical optimization methods: grid search, random search, and Bayesian optimization. The following hyperparameters were used to train the model: a learning rate of 0.3, a weight update rate of 0.2, and a training time of 50. The training data set consists of 10,800 maturity assessment examples, randomized responses to an existing questionnaire, and no human participants. The learning rate is the step size at each iteration that determines how quickly the model adapts to the problem. Momentum is the rate at which the weight is updated. And the training time is the number of epochs that need to be passed through the models [24].

3.3 Development of a model for assessing the security of information systems

3.3.1. Defining the base paradigm of the valuation model

Methods and systems using artificial intelligence (AI) can lead to unexpected results and can be modified to manipulate the expected results [25]. Therefore, the security of the AI itself is important. In particular, it is important:

- understand what needs to be protected (assets with specific AI threats),
- understand relevant data management models (including the development, evaluation, and protection of data and the learning process of AI systems),
- comprehensively manage threats across a multi-stakeholder ecosystem using common models and taxonomies,
- develop special controls to ensure the security of the AI itself.

For the correct formation of an intellectual system, it is important to follow a structural and methodological approach to understanding its various aspects [14,16]. Machine learning (ML) is a part of artificial intelligence. There are several learning models for ML algorithms: supervised, unsupervised, reinforcement, and partially supervised. The purpose of the reference model is to provide a conceptual framework that facilitates the allocation of ownership across different assets and provides a structured way to analyze relevant security threats. Data is one of the most valuable assets of artificial intelligence [5,26], therefore, before developing a model, it is important to fully define the business context for using an AI system, and collect data for analysis, and define controls [27]. The semi-supervised method is an average between supervised and unsupervised learning, according to the authors of [28–30], it allows achieve greater accuracy of the models.

In addition to choosing a model, we need to choose a training strategy for its modification and increase in efficiency. There are many training algorithms for error minimization, most of which are based on gradient descent. The backpropagation method is an iterative method based on the algorithm for updating multilayer perceptron scales by calculating stochastic gradient descent [31,32] to minimize neural network error. When this method is iterated, the error signals are distributed from the outputs to the inputs of the network. However, this method requires the use of a differentiated gear ratio. A cutting linear unit [33] or a rectified linear unit [34] (ReLU) is a differentiated gear ratio (activation function), which is mathematically defined as follows (2):

$$f(x)=max(0,x), \tag{2}$$

where x is the input value of the neuron.

According to the circuitry, it is an analog of a semi-periodic rectifier. This gear ratio was introduced for dynamic networks by Hahnloser and others in 2000 [35] with a biological basis and mathematical justification. ReLU is often used in computer vision and speech recognition tasks.

3.3.2. Data preconditioning for training

The input data for our experiment was provided by one of the Ukrainian companies as part of a joint research project with Taras Shevchenko National University of Kyiv. The data was generated by a questionnaire based on the comparison of ISO 27000 standards and ISO 21827:2008 standards to assess maturity for the specific purposes of this study.

The international standard ISO/IEC 27002:2013 [36] provides recommendations for the development and implementation of ISMS by organizations in terms of selecting and managing controls, taking into account existing risks. Contains a complete description and recommendations for implementing an ISMS (compared to ISO/IEC 27001:2013). The standard contains 14 clauses containing 35 main categories of information security and 114 controls, a list of which is presented in the ISO/IEC 27001 standard, Appendix A [37]. The order of the sections does not reflect their importance to a particular organization. The questionnaire was prepared to take into account all domains and controls of the ISO/IEC 27002:2013 standard. An example of the structure of ISO/IEC 27002:2013 controls is shown in Figure 3. A sample questionnaire (questionnaire fragment) is shown in Figure 4.

An expert (auditor) evaluates each specific security measure (columns 1-2) on a 6-point scale (0..5). Let A_j be an attribute that represents the evaluation of the jth security control. The attribute takes values in the range from 0 to 5. Mathematically, it can be defined as follows (3):

$$A_j \in I = \{0, \ldots, 5\}, \tag{3}$$

where A_j is the maturity score of the jth security measure with thresholds: 0 is the lowest and 5 is the highest maturity level. The number of attributes is equal to the number of corresponding security controls from the ISO/IEC 27001:2013 standards (may vary in the range of 0…700). The maturity mapping rule is described in Table 4.

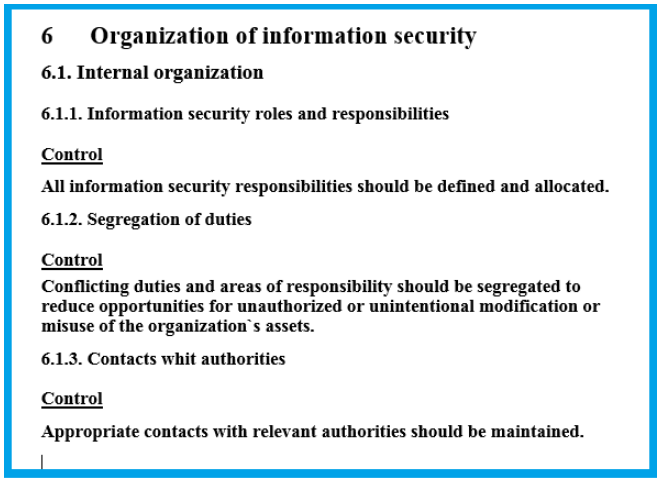

Figure 3: Sample structure of sections and controls in ISO 27002.

Table 4
Evaluation of the scope of ISO/IEC 27001:2017 security controls

Level	Value
not performed	0
performed informally	1
planned	2
well defined	3
quantitatively controlled	4
continuous improvement	5

The questionnaire has been prepared to consider the following 11 areas of ISO/IEC 27001, namely:

1. Information security policy
2. Organization of information security
3. Asset management
4. Security of human resources
5. Physical and environmental security
6. Communications and Operations Management
7. Access control
8. Acquisition, development, and maintenance of the information system
9. Information security incident management
10. Business continuity management
11. Compliance

The dataset consists of 10831 instances. The data instance consists of two parts, a set of security control scores (Vector 1 .. Vector 5) and an associated class. A fragment of the data set of the enterprise under study for assessing security is shown in Table 5. Vectors 1-5 represent assessments of the levels of maturity of information security processes. The rows of the table represent specific information security measures following the standard ISO 27002. The last column "Data status" can take one of 6 values (Table 4).

Table 5
Fragment of the data set of the studied enterprise for security assessment

Vector 1	Vector 2	Vector 3	Vector 4	Vector 5	Data status
3	5	0	2	1	Planned
5	2	2	1	3	Well-defined
4	4	5	3	0	Planned
2	2	2	4	5	Well-defined
3	4	5	3	3	Planned
5	1	5	4	0	Planned
4	1	2	0	5	Planned
5	3	1	1	0	Planned

A new class attribute has been added to the final data set to indicate that the control set meets a certain level of maturity.

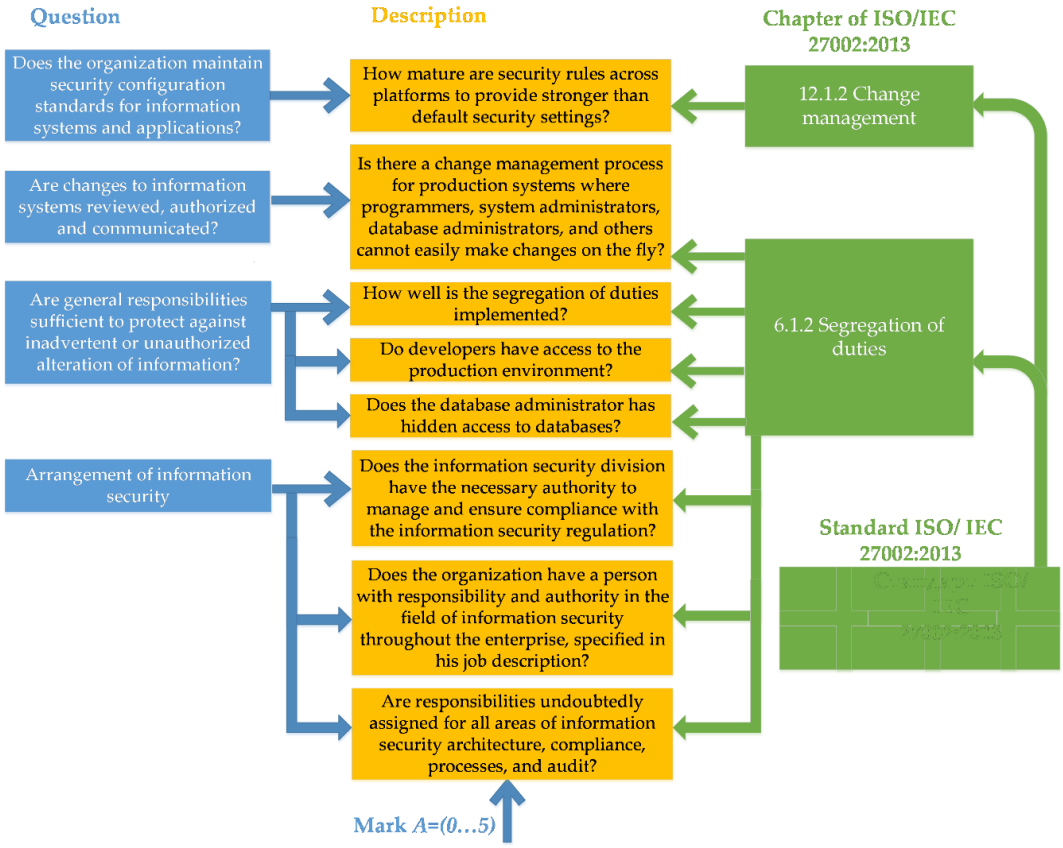

Figure 4: Sample questionnaire.

An example of input data is shown in Table 6. The columns of the matrix contain the assessment of the auditors for each security control. The data fragment of the input parameters of the model includes:

- Relations with suppliers (L1-L5)
- Management of information security incidents (M1-M2)
- Business continuity management (N1)
- Communication security (O1-O8

Table 6
Final dataset

Supplier Relationships						Information Security Incident Management		Business Continuity Management	Communications Security								
L1	L2	L3	L4	L5	L6	M1	M2	N1	O1	O2	O3	O4	O5	O6	O7	O8	Class
4	5	0	0	3	2	0	4	5	5	5	1	4	1	4	1	3	2
2	5	3	5	4	2	3	2	1	0	4	1	4	3	5	3	3	3
5	0	1	1	5	4	1	2	5	5	3	5	4	0	3	3	2	2
0	3	1	4	3	5	2	1	4	4	5	5	1	4	3	2	0	3
2	4	4	4	1	3	1	4	5	3	3	3	2	5	5	1	5	2
3	1	3	3	3	2	5	4	5	2	5	5	1	4	2	0	1	3
2	1	5	3	4	5	0	5	1	1	0	0	0	2	4	2	0	2
0	1	5	4	4	1	1	1	5	2	0	4	1	2	5	5	2	2
3	3	1	3	5	1	4	4	3	0	5	4	2	3	1	4	1	2
2	3	4	1	3	4	0	4	3	4	4	2	2	5	4	3	4	3
4	5	3	2	2	0	1	3	1	0	1	4	1	5	4	4	0	3

3.4. Training process

For the training process of the neural network to assess the information security maturity of the system the application was developed using the WEKA (Waikato Knowledge Analysis Framework) tool (Figure 5), and the requirements for the training parameters of the neural network to assess the maturity of the information security of the system are in Table 7. To check the accuracy of the model, the initial set was divided into smaller ones: 100 000, 250 000, 500 000, and 1 000 000 respectively.

Table 7
Requirements for neural network training parameters for assessing the information security maturity of the system

№	Parameter	Value
1	Learning rate	0 to 1, the default is 0.3
2	Momentum rate	0 to 1, the default is 0.2
3	Number of epochs to train	default is 500 (used 50 due to data redundancy)
4	Percentage size of the validation set used to complete training	0 to 100, default is 0
5	A value used to generate the random number generator	≥0 and less long
6	Number of hidden layers	comma separated list of natural numbers or letters 'a' - (attributes + classes) / 2, 'i' - attributes, 'o' - classes, 't' - attributes + classes. The default is 'a'
7	Required burst size for prediction	default is 100

Table 8
Statistical parameters of training samples

Training sample size N	Expected value	Standard deviation
10910	2.581118	1.583218
049	2.712107	1.595302

A graphical representation of the frequency distribution of data instances in the set of training materials is shown in Figure 6. The results are statistically processed, and the parameters are shown in Table 8. Let's check if the sample complies with the normal distribution law. As shown in Figure 6 (a) the incoming data sequence has the properties of a normal distribution. The histogram and the normal distribution function built in the Excel package are shown in Figure 6: (b) shows the case for N = 10910, (c) shows the case for N = 1049.

```
public Classifier buildClassifier(Instances traindataset) {
    MultilayerPerceptron m = new MultilayerPerceptron();

    m.setGUI(true);
    m.setValidationSetSize(80);
    m.setBatchSize("100");
    m.setLearningRate(0.3);
    m.setSeed(0);
    m.setMomentum(0.2);
    m.setTrainingTime(500);//epochs
    m.setNormalizeAttributes(true);

    m.setHiddenLayers("11");

    try {
        m.buildClassifier(traindataset);

    } catch (Exception ex) {
        Logger.getLogger(ModelGenerator.class.getName()).log(Level.SEVERE, msg: null, ex);
    }
    return m;
}
```

Figure 5: Implementation of the neural network training algorithm for assessing the maturity of the information security of the system.

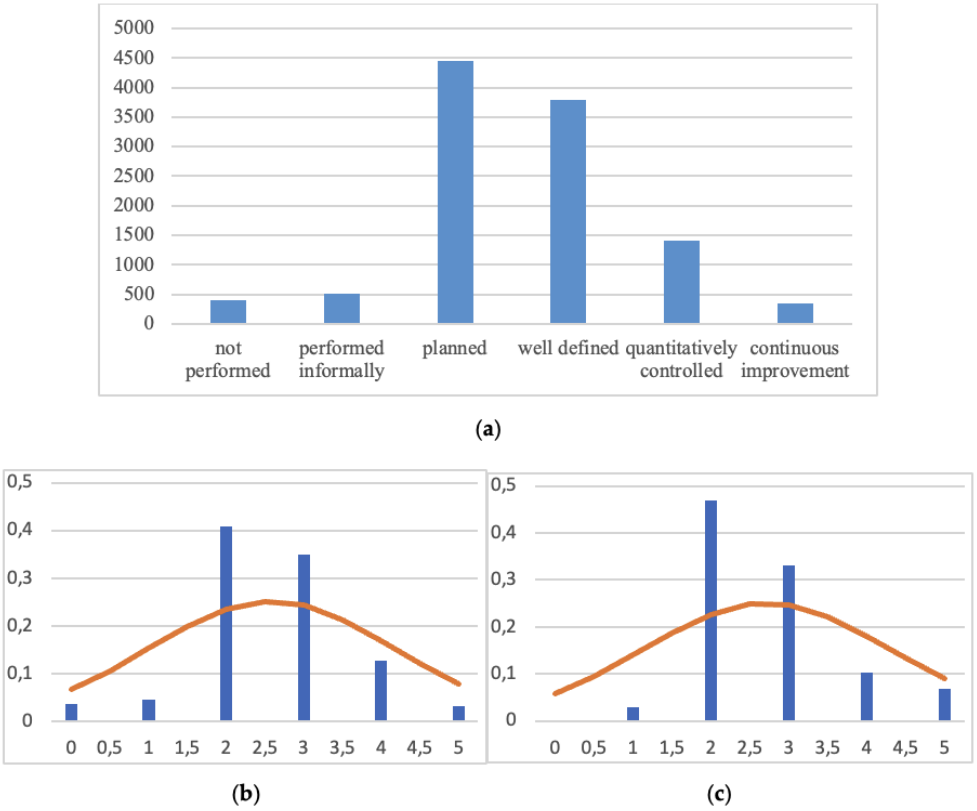

Figure 6: Distribution of data instances in the training sample (frequency of elements in the response data): (a) histogram in natural units; (b) normal distribution histogram with a total of 10910 records; (c) histogram with a normal distribution with a total of 1049 records.

3.5. Model implementation

3.5.1. Synthesis of models

For the above reasons, it was decided to build a maturity assessment model based on ANN (artificial neural network) of forwarding signal propagation with error backpropagation, in particular, a multilayer perceptron. A multilayer perceptron (MLP) is a type of organization of a neural network of direct signal propagation [38]. The typical perception is that of a fully saturated network, which

means that each node in one layer has a certain weight concerning each node in the next layer. Typically, it consists of an input layer, hidden layers, and an output layer, as shown in Figure 7.

The model was synthesized based on an artificial neural network of forwarding propagation with backpropagation, MLP, which consists of three layers of nodes: an input layer, a hidden layer, and an output layer. The initial weights are arbitrary. The input layer for an artificial neural network consists of the control objectives implemented in the organization. It is represented by input variables. The output of an artificial neural network is the final value of the maturity level, that is, a verdict or a prediction given the input data. Hidden layers perform certain transformations on the input data. The node in the hidden layer uses a weighted linear sum and, in particular, an activation function. The neural network consists of the management objectives implemented in the organization.

Except for the input nodes, each node is a neuron using a non-linear activation function. MLP uses a supervised learning method called backpropagation for learning. ReLU is used as an activation function, it is used to determine the output of the network. A maturity model can also be defined as a structured set of elements that describe the characteristics of efficient processes or products [28]. Thus, the information security maturity level (ISML) will be calculated according to the formula:

$$ISML = \sum_{i=1}^{n} W(C_i)\, ISML(C_i), \tag{4}$$

where $W(C_i)$ is the weight of the ith control, n is the number of controls, $ISML(C_i)$ is defined according to the rule described in Table 2.

$$\sum_{i=1}^{n} W(C_i) = 1, \tag{5}$$

Let the initial control weights be defined as:

$$W(C_1) = W(C_2) = \ldots W(C_n) = \frac{1}{n}, \tag{6}$$

The MLP algorithm is implemented in the open-source software WEKA [39], released under the GNU General Public License. WEKA was developed at the University of Waikato (New Zealand) for research purposes. It provides a set of machine learning tools and algorithms for data mining tasks. It contains tools for data preprocessing, classification, regression, clustering, association extraction rules, visualization, and implementation of several machine learning algorithms. WEKA is a free Java class library. WEKA contains an API (Application Programming Interface) that implements existing learning algorithms with minimal settings. So, the functions of the model generator are present in the following code fragments (Figure 8).

This software supports ARFF (Attribute Relationship File Format) data import, an ASCII text file that describes a data model using attributes and data instances. ARFF files are ordered in the following order: relation name, attribute list, and data instances presented line by line [39]. The program has created a file with the model extension. The average model generation time for this data set is 400 seconds. This file will be used to classify new data. The interface of the Weka system, which demonstrates the process of training a neural network with a dataset of 1049 records, is shown in Figure 9. The ReLU activation function is used to determine the output of the network.

3.5.2. Summary

Several studies [17,20–23,40–46] can be used to determine compliance with ISO/IEC 27001:2013. However, no maturity model satisfies the requirements of ISO/IEC 27001. Accordingly, if existing

models fail to solve the problem, a new maturity model should be developed. First, the basic paradigm of the maturity model was developed, as a result of which the apparatus of neural networks of forwarding signal propagation and error backpropagation was chosen for model synthesis. In addition, a list of requirements for each maturity level was prepared following the requirements of ISO/IEC 27001 and ISO/IEC 27002 standards. For further training and solving the classification problem, a supervised learning algorithm, backpropagation of errors to correct the internal parameters of the model, and activation of ReLU functions. The next step was the development of an algorithm for preliminary data preparation for training and data preparation itself. To do this, a questionnaire was generated taking into account all domains and ISO/IEC 27002:2013 management tools, and data was also generated.

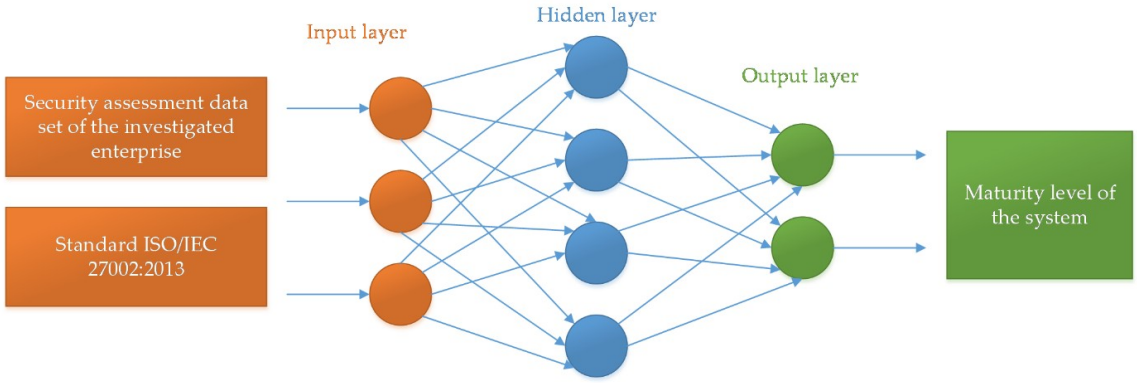

Figure 7: Multilayer perceptron with one hidden layer.

The last step was the synthesis and training of the model using the apparatus of neural networks. In addition to the previously mentioned, the model has the following configuration (Table 9).

Table 9
Characteristics of the ANN model

Characteristic	Value
Number of neurons in the input layer	114
Number of neurons in the hidden layer	60
Number of neurons in the output layer	6
Learning rate	0.3
Weight update frequency	0.2
Studying time	50
Number of maturity assessment examples in the training dataset	10 831

4. Results

4.1. Validating the adequacy of the model

The adequacy analysis made it possible to check the degree of correspondence of the model to a real system with a set of certain properties [47] and was carried out in several stages:

1. Evaluation of control coverage using ontological deficits by Wand and Weber [48].
2. Evaluate the coverage of controls and requirements of ISO/IEC 27001 by the ISMS maturity model using the methodology used when comparing other models.

4.2. Model adequacy analysis by Wand and Weber method

Wand and Weber define the ontological evaluation of the method to identify four ontological flaws: incompleteness, redundancy, excess, and overload. An ontological assessment of the scope of

ISO/IEC 27001 requirements of the proposed ISMS maturity model is presented in Table 10. Based on the results of the analysis, the model is complete as it fully covers IEC 27001 controls. There is no redundancy. However, the ISO/IEC 27001 requirement "4.2.3-d)" has been overloaded because we believe it describes the requirements for three different activities. As a result, three different evaluation criteria were created for this requirement. Finally, the ISMS maturity model covers all the requirements detailed in clause 4 of ISO/IEC 27001, which means that the total score on the same scale is 20.

Table 10
ISO/IEC 27001 coverage of the proposed Wand and Weber ISMS maturity model

Deming cycle stages	Proposed maturity model controls	ISO/IEC 27001 Requirement	Estimation according to the Wand and Weber method
Plan	Maturity level: Planned		
	Define the scope and limits of ISMS	4.2.1 – a)	Complete
	Develop an ISMS policy	4.2.1 – b)	Complete
	Define an approach to risk assessment	4.2.1 – c)	Complete
	Perform risk identification	4.2.1 – d)	Complete
	Risk analysis and assessment	4.2.1 – e)	Complete
	Determination of risk treatment options	4.2.1 – f)	Complete
	Define objectives and criteria controls for risk treatment	4.2.1 – g)	Complete
	Obtain permission to approve residual risks	4.2.1 – h)	Complete
	Obtain permission for ISMS implementation and function	4.2.1 – i)	Complete
	Preparation of a statement of applicability	4.2.1 – j)	Complete
Do	Maturity level: Well-defined		
	Make a risk management plan	4.2.2 – a)	Complete
	Implement a risk management plan	4.2.2 – b)	Complete
	Implementation of selected controls	4.2.2 – c)	Complete
	Determine how to measure the effectiveness of controls	4.2.2 – d)	Complete
	Implement training and awareness programs	4.2.2 – e)	Complete
	Manage the operation of the ISMS	4.2.2 – f)	Complete
	ISMS resource-management	4.2.2 – g)	Complete
	Implement procedures and other controls to be able to promptly detect security events and respond to security incidents	4.2.2 – h)	Complete
Check	Maturity level: Quantitatively controlled		
	Perform monitoring and review procedures as well as other controls	4.2.3 – a)	Complete
	Conduct regular reviews of the ISMS performance	4.2.3 – b)	Complete
	Measure the effectiveness of controls	4.2.3 – c)	Complete
	Review risk assessment	4.2.3 – d)	Overwhelmed
	View residual risks	4.2.3 – d)	Overwhelmed
Act	Maturity level: Continuous improvement		
	Implement identified improvements in ISMS	4.2.4 – a)	Complete
	Take appropriate corrective and precautionary measures	4.2.4 – b)	Complete
	Inform all stakeholders about ISMS actions and improvements	4.2.4 – c)	Complete
	Ensure that improvements achieve the intended goals	4.2.4 – d)	Complete

4.3. Model testing on 5 real organizations

After the first two stages of evaluation, we evaluated five real organizations (Table 11). For each of these five organizations, an ISMS maturity assessment was carried out and the result is shown in

Table 12. In this table, "+" means a satisfactory assessment (3 points or more), an empty cell – an unsatisfactory assessment. The last row shows the final maturity level for each organization.

```
public String evaluateModel(Classifier model, Instances traindataset, Instances testdataset) {
    Evaluation eval = null;
    try {
        // Evaluate classifier with test dataset
        eval = new Evaluation(traindataset);
        eval.evaluateModel(model, testdataset);
    } catch (Exception ex) {
        Logger.getLogger(ModelGenerator.class.getName()).log(Level.SEVERE,  msg: null, ex);
    }
    return eval.toSummaryString( title: "",  printComplexityStatistics: true);
}

public void saveModel(Classifier model, String modelpath) {

    try {
        SerializationHelper.write(modelpath, model);
    } catch (Exception ex) {
        Logger.getLogger(ModelGenerator.class.getName()).log(Level.SEVERE,  msg: null, ex);
    }
}
```

```
public Instances loadDataset(String path) {
    Instances dataset = null;
    try {
        dataset = ConverterUtils.DataSource.read(path);
        if (dataset.classIndex() == -1) {
            dataset.setClassIndex(dataset.numAttributes() - 1);
        }
    } catch (Exception ex) {
        Logger.getLogger(ModelGenerator.class.getName()).log(Level.SEVERE,  msg: null, ex);
    }

    return dataset;
}
```

Figure 8: Model generator functions in Weka Software.

Table 11
List of organizations for model testing

Organization	Type of ownership	Description
Organization "1"	Government agency	Promotion and development of administrative modernization
Organization "2"	It is part of the business sector of the government of the country	Production and supply of goods and services requiring high-security standards: coins, banknotes, documents
Organization "3"	State higher education institution	About 13,700 students study
Organization "4"	Government agency	Scientific and technical research and development
Organization "5"	Private organization	Software development and maintenance

The left part of the table contains codes of control actions for implementation of the safety measure (see Table 3). Table 12 shows that all safety measures are implemented only in Organization 1 (state administrative institution). The majority of measures (25 out of 30) were implemented in

Organization 4 (research institute), while the measures of Group 5 (Improving) were not implemented at all. The smallest number of activities (14 out of 30) is realized in organization 3 (higher education institution), probably, it is connected with the large number of participants in the process and premises and weak manageability of the enterprise.

It can also be noted that the activities of Group 2 (Planning) are implemented at all 5 enterprises, while the activities of Group 5 (Improving) are fully implemented at Enterprise 1 (governmental institution) and partially at Enterprise 5 (software developer).

To achieve a certain level of maturity, an organization must meet all the criteria for that particular level and all levels below [14], for example, an organization at maturity level 3 meets all the criteria for maturity levels 1, 2, and 3.

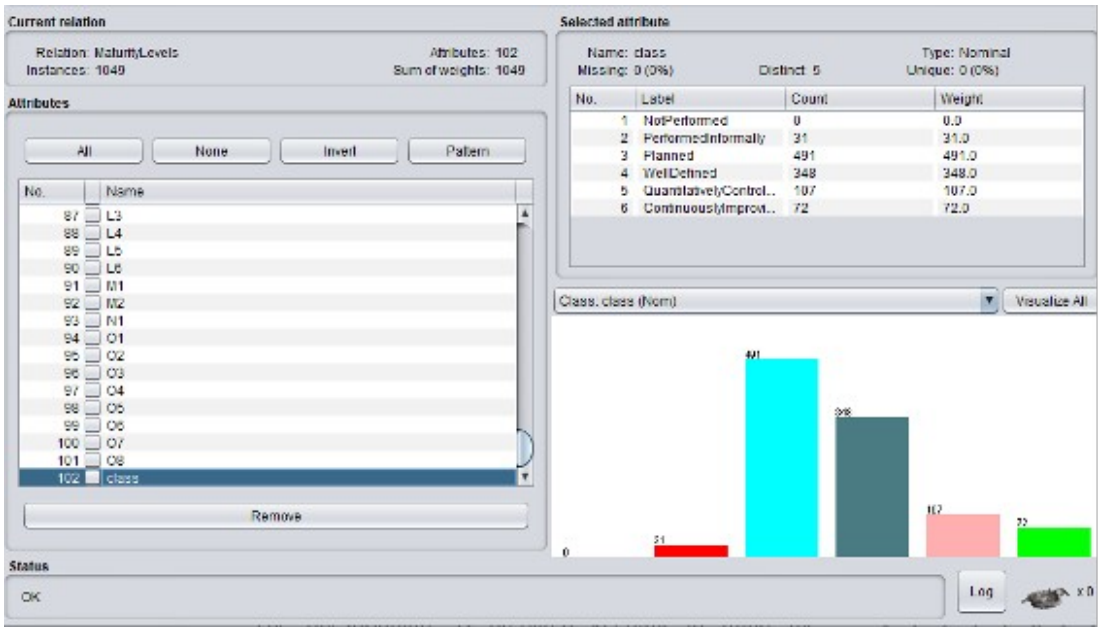

Figure 9: The interface of the Weka system shows the process of training a neural network.

Table 12
The result of assessing the maturity of enterprises using the proposed ISMS maturity model

Control	1	2	3	4	5
2.1	+	+	+	+	+
2.2	+	+	+	+	+
2.3	+	+	+	+	+
2.4	+	+	+	+	+
2.5	+	+	+	+	+
2.6	+	+	+	+	+
2.7	+	+	+	+	+
2.8	+	+	+	+	+
2.9	+	+	+	+	+
3.1	+	+		+	+
3.2	+	+		+	+
3.3	+	+		+	+
3.4	+	+		+	+
3.5	+	+	+	+	+
3.6	+	+	+	+	+
3.7	+	+	+	+	+
3.8	+	+		+	+
4.1	+			+	+
4.2	+			+	+
4.3	+		+	+	+

4.4	+			+	
4.5	+			+	+
4.6	+	+		+	
4.7	+	+		+	
4.8	+	+	+	+	
4.9	+			+	+
5.1	+				+
5.2	+				+
5.3	+				
5.4	+				
Maturity level	5	3	2	4	3

4.4. Validating model accuracy using statistical methods

4.4.1. Basic concepts for assessing the accuracy of the constructed model

Accuracy (significance) is a statistical metric showing the percentage of positive results classified correctly. The low accuracy value is usually associated with a large number of false positive classifications [49]. In addition, the following statistical metrics are used to evaluate models: recall (sensitivity), F-measure (takes values from 0 to 1), Matthew Correlation Coefficient (MCC), or Phi coefficient is used in machine learning as an indicator of the quality of binary classifications, performance receiver (ROC), accuracy-recall curve (PRC), kappa statistics (describes the accuracy of the classifier) [49].

4.4.2. Model accuracy test results using statistical methods

To test the accuracy of the model, the original set was divided into smaller parts: 70% for training, 15% for the control set, and 15% for the test set. First, a cross-validation method was performed to determine performance statistics for the model. The model was then trained again but used 100% of the data set to get the most accurate model to get a robust classification model. A generalized error matrix is shown in Table 13.

Table 13
The result of the analysis of the accuracy of the model

Characteristic	Test 1	Test 2	Test 3	Test 4	Test 5
Training sample size	10000	3000	5000	1500	2000
Classified correctly (percentage)	99.65	97.74	98.31	95.24	96.07
Misclassified (percentage)	0.35	2.27	1.70	4.77	3.94
Kappa coefficient	0.995	0.972	0.980	0.952	0.958
Average absolute error	0.002	0.003	0.002	0.005	0.003
The mean square error	0.033	0.073	0.054	0.954	0.086
Relative error (percentage)	0.88	0.63	0.76	0.50	0.59
The relative mean squared error (%)	9.75	12.31	10.25	14.02	12.98

The inconsistency matrix (Table 14) is used to evaluate the performance of the classification model [49]. It provides information on classification inconsistencies, which can also be used to identify a possible trend in existing errors. The accuracy of the estimate is given in Table 15.

So, the trained model successfully classified 99.649% of the dataset, the reliability of the classifier is 0.9949, which can be interpreted as almost perfect data agreement, and the root means the square relative error is 9.748%. Other model results include true positive rate – 0.996, false-positive rate – 0.001, accuracy – 0.996, completeness – 0.996, f-measure – 0.996, Matthew's correlation coefficient – 0.962–1, ROC area – 0.998, PRC area – 0.995.

Table 14
Gap matrix

Level 0	Level 1	Level 2	Level 3	Level 4	Level 5	Classified as
208	10	0	0	0	0	Level 0
6	526	7	5	0	0	Level 1
0	0	4462	0	0	0	Level 2
0	0	10	3847	0	0	Level 3
0	0	0	0	1410	0	Level 4
0	0	0	0	0	340	Level 5

Table 15
Accuracy by class

Class	0	1	2	3	4	5
True positive	0.954	0.967	1	0.997	1	1
True negative	0.001	0.001	0.003	0.001	0	0
Accuracy	0.972	0.981	0.996	0.999	1	1
Completeness	0.954	0.967	1	0.997	1	1
F-Measure	0.963	0.974	0.998	0.998	1	1
MCC	0.962	0.973	0.997	0.997	1	1
ROC area	1	0.991	0.998	0.998	1	1
PRC area	0.987	0.979	0.994	0.997	1	1

5. Discussion and perspectives

We assessed the performance of each of the evaluation controls, which in turn allowed us to determine the level of maturity of the ISMS for each of the five organizations. The results of the assessment in Table 12 showed that the maturity model correctly identified the level of maturity, and they are consistent with the perception of the maturity of the ISMS implemented in the organization. The results were used by organizations to create improvement plans specifically tailored to their organizational context. The disparity matrix in Table 14 shows that there are misclassifications for the first three classes, which can be caused by an insufficiently balanced dataset. This means that this dataset should be adjusted to achieve better results in future studies. The given values in Table 15 indicate that the trained model describes a real manual process for assessing the maturity of information security at an acceptable level, and it can be recommended for usage in the process of a real ISMS audit.

Thus, a maturity model of ISMS processes has been developed under the requirements and recommendations of ISO/IEC 27001:2013 and ISO/IEC 27002:2013 using the apparatus of neural networks of forwarding propagation of signals and backpropagation of errors. The practical significance of the work lies in the fact that the results can be applied in the activities of a particular institution to improve the system for assessing the security of information systems. The proposed method makes it possible to automate the solution of tasks assigned to an expert: assessing the compliance of information systems with security requirements and making a decision on their use.

Moreover, this approach will be very useful when using other security frameworks, such as NIST (National Institute of Standards and Technology) SP (Special Publication) 800 series and, in particular, NIST SP 800-53 [50]. There are many requirements and a rich set of controls to consider. Therefore, the application of the developed model can significantly reduce the time spent by experts. For a deeper analysis of the usefulness of the maturity model and its improvement, it is proposed to

evaluate the use of the ISMS maturity model in various industries. This will lead to a more general and objective validation of the model and will allow for cross-industry benchmarking.

6. Conclusions

None of the existing maturity models satisfactorily take into account the requirements of ISO/IEC 27001 [37]. Accordingly, it was decided to develop a new maturity model using forward signal propagation and error backpropagation neural networks. The list of requirements for each maturity level has been prepared following the requirements of ISO/IEC 27001 and ISO/IEC 27002.

For further training and solving the classification problem, a supervised learning algorithm, error backpropagation to correct the internal parameters of the model, and the ReLU activation function were chosen. The effectiveness of this model of using artificial neural networks for solving the problem is substantiated. The ISMS maturity model was assessed by a multi-aspect method and statistical means. The proposed model is found to be complete as it fully covers IEC 27001 controls. There is no redundancy or redundancy. The trained model describes a real non-automated process of assessing the maturity of information systems at an acceptable level of security and can be recommended for use in the process of a real ISMS audit.

The model developed from this study can be used as part of a decision support system to enable cybersecurity decision-makers to:

1. Make informed decisions, choosing the best option to mitigate certain vulnerabilities/threats and maintain business continuity.
2. Analyze the strengths and weaknesses of the ISMS processes.
3. Develop a strategy for the evolutionary improvement of the capabilities, efficiency, and effectiveness of the ISMS [16,26].

As a result, it will also help to reduce the time and financial resources for assessing the security of enterprises.

Declaration on Generative AI

The authors have not employed any Generative AI tools.

References

[1] ISO/IEC 27000 Information security management systems. Overview and vocabulary, 2013.

[2] HIPAA. Health Insurance Portability and Accountability Act of 1996. https://web.archive.org/web/20171227202818/http: //legalarchiver.org/hipaa.htm.

[3] Babenko, T.; Hnatiienko, H.; Vialkova, V. Modeling of the integrated quality assessment system of the information security management system, 2021.

[4] Zgurovskyi, M. Technology foresight of Ukrainian economy in the medium (up to 2020) and long term (until 2030) horizons. According to the materials of the scientific report at the meeting of the Presidium of NAS of Ukraine, November 4, 2015, Visn. Nac. Akad. Nauk Ukr.; 2016;1:67-68. DOI: 10.15407/visn2016.01.057.

[5] Hnatiienko, H. Choice Manipulation in Multicriteria Optimization Problems, 2019.

[6] Miloslavskaya, N.; Sagirov, R. Review of Information Security Processes of Maturity Models, 2015.

[7] Polyanichko, M. Application of the maturity model to counter insider threats to information security, 2019. https://doi.org/10.2 3670/IRJ.2019.82.4.010.

[8] Proença, D.; Borbinh, J. Maturity Models for Information Systems – A State of the Art, 2016. https://doi.org/10.1016/j.procs.20 16.09.279.

[9] Uzoka, E. A CMM Assessment of Information Systems Maturity Levels in Botswana, September 2010.

[10] Han, W.; Sun, X.Y.; He, C.; Tang, L.L.; Kumari, S. A Novel Network Security Data Resource Description Standard, 2022.
[11] Li, W.; Yan, W.; Ding, Q.; Zhang, R.; Chen, Y.C. Discrete Synchronization Method for Continuous Chaotic Systems and Its Application in Secure Communication, 2020.
[12] Hrechko, V.; Babenko, T. Defining the meaningful attributes of network traffic, 2017. https://doi.org/10.1109/WorldS451998.20 21.9514019.
[13] Borisov, I. Overview of the level of maturity of information security processes: about trends and methodologies, 2018.
[14] Babenko, T.; Hnatiienko, H.; Bigdan, A. Model for determining the protection level of a complex system, 2022.
[15] Jebb, A.; Parrigon, S.; Woo, S. Exploratory data analysis as a foundation of inductive research, 2017. https://doi.org/10.1016/j. hrmr.2016.08.003.
[16] Hrechko, V.; Hnatienko, H.; Babenko, T. An intelligent model to assess information systems security level, 2021. https://doi.org/10.1109/WorldS451998.2021.9514019.
[17] The Department of Energy, D. Cybersecurity Capability Maturity Model (C2M2), Version 1.1, 2014.
[18] Garba, A.; Siraj, M.; Othman, S. An Explanatory Review on Cybersecurity Capability Maturity Models, 2020.
[19] Dubois, E.; Heymans, P.; Mayer, N.; Matulevicius, R. A Systematic Approach to Define the Domain of Information System Security Risk Management, 2010. https://doi.org/10.1007/978-3-642-12544-7_16.
[20] Team, S.P. System Security Engineering Capability Maturity Model (SSE-CMM): Model Description Document, Version 3.0, 2003.
[21] White, G. The community cyber security maturity model, 2011. https://doi.org/10.1109/HICSS.2007.522.
[22] Group, T.O. Open Information Security Management Maturity Model (O-ISM3), 2011.
[23] ISACA. COBIT 2019 Framework: Introduction and Methodology, 2018.
[24] Yang, L.; Shami, A. On hyperparameter optimization of machine learning algorithms: Theory and practice, 2020.
[25] ENISA. AI Cybersecurity Challenges. Threat Landscape for Artificial Intelligence, December 2020. https://doi.org/10.2824/23 8222.
[26] O.A. Manankova, M.Z. Yakubova, M.A. Rakhmatullaev, and A.S.Baikenov, “Simulation of the Rainbow Attack on the SHA-256 Hash function,” J. of Theoret. and Appl. Inf. Tech., vol. 101, no. 4, pp. 1594–1603, 2023.
[27] Sarker, I. Deep cybersecurity: a comprehensive overview from neural network and deep learning perspective, 2021.
[28] Dixit, P.; Silakari, S. Deep learning algorithms for cybersecurity applications: A technological and status review, 2021. https://doi.org/10.1016/j.cosrev.2020.100317.
[29] Xin, Y. Machine learning and deep learning methods for cybersecurity, 2018. https://doi.org/10.1109/ACCESS.2018.2836950.
[30] T. Velyamov, A. Kim, O. Manankova, Modification of the Danzig-Wolf Decomposition Method for Building Hierarchical Intelligent Systems, Int. J. of Adv. Comput. Sci. and Appl., vol.15, no.7, pp. 1160–1167, 2024. Doi: 10.14569/IJACSA.2024.01507113.
[31] Werbos, P. Beyond regression: New tools for prediction and analysis in the behavioral sciences, 1974.
[32] Rumelhart, D.; Hinton, G.; Williams, R. Learning Internal Representations by Error Propagation, 1986.
[33] LeCun, Y.; Bengio, Y.; Hinton, G. Deep learning, 2015. https://doi.org/10.1038/nature14539.
[34] Goodfellow, I.; Bengio, Y.; Courville, A. Deep learning, 2016.
[35] Hahnloser, R.; Sarpeshkar, R.; Mahowald, M.; Douglas, R.; Seung, H. Digital selection and analogue amplification coexist in a cortex-inspired silicon circuit, 2000. https://doi.org/10.1038/35016072.

[36] International Standard ISO/IEC 27002. Information technology – Security techniques – Code of practice for information security controls, 2013.
[37] The new ISO/IEC 27001:2022 standard. https://www.bsigroup.com/en-GB/iso-27001-information-security/ISOIEC-27001-Revision/, 2022.
[38] Dixit, M. An overview of deep learning architectures, libraries and its applications areas, 2018. https://doi.org/10.1109/ ICACCCN.2018.8748442.
[39] Bouckaert, R.R. WEKA manual for version 3-9-1. University of Waikato, Hamilton, New Zealand, 2016.
[40] Halvorsen, C.; Conradi, R. A taxonomy to compare SPI frameworks, 2001. https://doi.org/10.1007/3-540-45752-6_17.
[41] Palko, D.; Myrutenko, L.; Babenko, T.; Bigdan, A. Model of Information Security Critical Incident Risk Assessment, 2021. https://doi.org/10.1109/PICST51311.2020.9468107.
[42] ISF. Time to grow using maturity models to create and protect value. Information Security Forum ISF, 2014.
[43] Practices, A.G.B. RESILIA Practitioner Examination Syllabus. "https://www.scribd.com/document/675109709/RESILIA-Foundation-2015-Syllabus", June 2015.
[44] Matthew, J. Advancing Cybersecurity Capability Measurement Using the CERT – RMM Maturity Indicator Level Scale: Version 1.1. Carnegie Mellon University, 2013. https://doi.org/10.1184/R1/6571847.v1.
[45] Z. Ayan, B. Alimzhan, M. Olga, Z. Timur, and Z.Toktalyk, Quality of service management in telecommunication network using machine learning technique, Indonesian J. of Electr. Eng. and Comput. Sci., vol. 32, no. 2, pp. 1022–1030, 2023. doi: 10.11591/ijeecs.v32.i2.pp1022-1030.
[46] Rea-Guaman, A.; Sánchez-García, I.; San Feliu, T.; Calvo-Manzano, J. Maturity models in cybersecurity: a systematic review, 2017. https://doi.org/10.23919/CISTI.2017.7975865.
[47] Hevner, S.C. Design Research in Information Systems: Theory and Practice, 2010. https://doi.org/10.4236/ib.2010.22013.
[48] Wand, Y.; Weber, R. On the ontological expressiveness of information systems analysis and design grammars, 1993, https://doi.org/https://doi.org/10.1111/j.1365-2575.1993.tb00127.x.
[49] Portugal, I.; Alencar, P.; Cowan, D. The use of machine learning algorithms in recommender systems: A systematic review, 2018. https://doi.org/10.1016/j.eswa.2017.12.020.
[50] National Institute of Standards and Technology. NIST Special Publication 800-53 Rev. 5: Security and Privacy Controls for Information Systems and Organizations, 2020.