ORGANIZATION INFORMATION SECURITY AUDIT ALGORITHM

[1]Kholimtaeva I.U., [2]Eshniyozov T.T.
[1]Senior teacher Tashkent University of Information Technologies
[2]Intern teacher at Tashkent university of Information Technologies
https://doi.org/10.5281/zenodo.10143811

Abstract. *In this article, an information model of conducting a cyber security audit of information systems based on the results of research and analysis of the means and methods of conducting a cyber security audit in organizations is proposed. This model meets the requirements of international standards and legal acts.*
Keywords: *audit, data array, incident and protection system.*

Implementation of complex work on information security audit is associated with a large amount of analyzed data, risk assessment and their presentation in the form of specific documents. In addition, there is the task of looking for resource vulnerabilities and analyzing the protection of information systems in general.

An information model is used to represent the main information objects, their properties, and the relationships between them.

An information model of the information technology (IT) cyber security audit process built using IDEF1X technology is presented in Figure 1.

IDEF methodology (Integrated DEFinition) is a view of any system being studied as a set of interacting and interconnected blocks that reflect the processes, operations, actions occurring in the studied system. In the IDEF methodology, three levels of detail are distinguished when describing processes:

IDEF0 – formalizes processes taking into account their functions, hierarchy and logical relationships between them;

IDEF1 – formalizes information processes taking into account their structure and interactions;

IDEF2 – formalizes the processes in the same way as IDEF0, taking into account the dynamics of transition of processes over time;

IDEF3 formalizes processes in the same way as IDEF0, in which each process can be further divided into separate functional blocks necessary for a detailed description of technological operations;

IDEF4 – formalizes processes based on the object-oriented approach, later this theoretical approach SOA (Service-Oriented Architectures) is the basis of practical concept.

The development of an information model allows for a visual and effective representation of the entire mechanism of the IT cyber security audit process. Conducted analysis of AT AX audit functions made it possible to compile the necessary information for support, distinguish the main stages of the audit, monitor the dynamics of information and resources.

The components of the IT cyber security audit information model and the relationships between them can be described as follows:

Components of an information model:

1. Audit organization; 2. Normative base; 3. IT cyber security audit information; 4. IT cyber security audit report

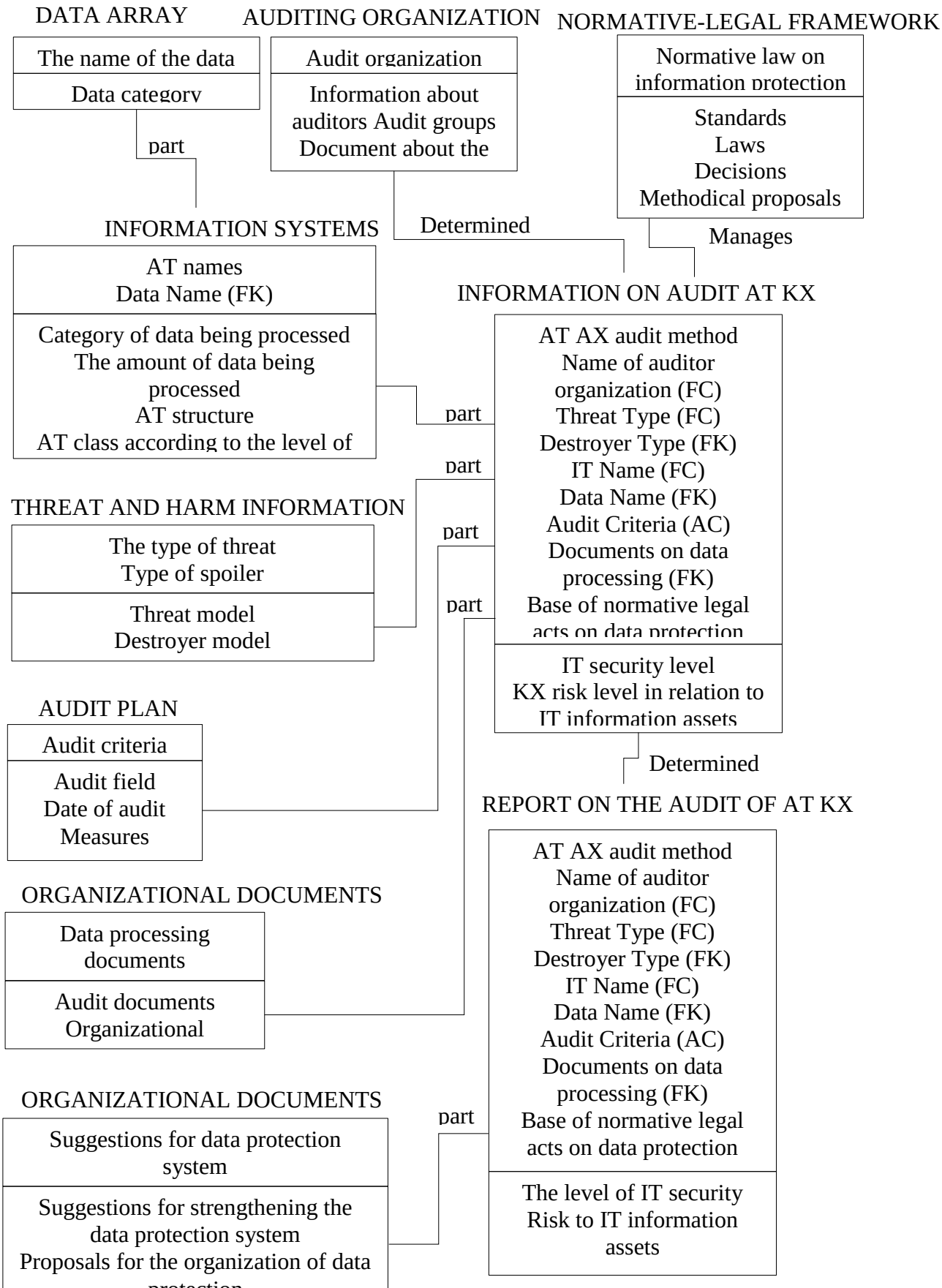

Figure 1. IT cyber security audit information model

Relationships between the components of the information model:

- "Information on IT cyber security audit" component consists of: information system, information about threats and criminals, audit plan and organizational documents;
- the list of recommendations is part of the IT cyber security audit report;
- the data array is a part of the information system;
- the audit organization defines the module "Information on IT cyber security audit", and the normative base regulates this module;
- IT cyber security audit report is defined with information about IT cyber security

The scheme depicted in Figure 2. Own DSt ISO/IEC 27007:2015 Information technology. Methods of ensuring security. Management guidelines for conducting audits in information security management systems. developed on the basis of This method demonstrates the use of the Plan - Do - Check - Take Action cycle.

The step/substep numbers are calculated according to the respective step/substeps of this standard.

Stage 1. Audit program management includes:

1.1. Determining the objectives of the audit program;

1.2. Identify and assess risks and opportunities associated with the audit program;

1.3. Developing an audit program, determining the roles and responsibilities of individuals for the audit program, their qualifications, as well as its size and resources;

1.4. Implementation of the audit program. In this sub-stage, the objectives, areas and criteria for a specific audit are determined, the selection and determination of audit methods, the selection of audit team members, the transfer of responsibility for a specific audit to the head of the audit team, the management of the results of the audit program, as well as the management and storage of audit program records are carried out;

1.5. Audit program monitoring;

1.6. Analysis and improvement of the audit program.

Stage 2. Conducting an audit consists of the following sub-stages:

2.1. Organization of audit. At this sub-stage, contact is established with the organization to be studied and opportunities for conducting an audit are determined;

2.2. Preparing for an audit. At the preparatory stage, the analysis of documented information, planning of the audit, then the distribution of work among the members of the audit team and the preparation of documented information for the audit are carried out;

2.3. Auditing. The audit process itself begins with defining the roles and responsibilities of accompanying observers, followed by an initial meeting and analysis of documented data during the audit. The next step is data collection and verification. At the end, the audit conclusions are formed, the final conclusions on the audit are prepared and the final meeting is held;

2.4. Preparation and distribution of the audit report;

2.5. Completion of the audit;

2.6. Further actions on audit results.

The following actions are performed when conducting a cyber security audit:

2.1. Organization of audit.

2.1.1 Contact with the audited organization is established.

1.1.2 Audit opportunities are identified

2.2. Preparing for the audit.

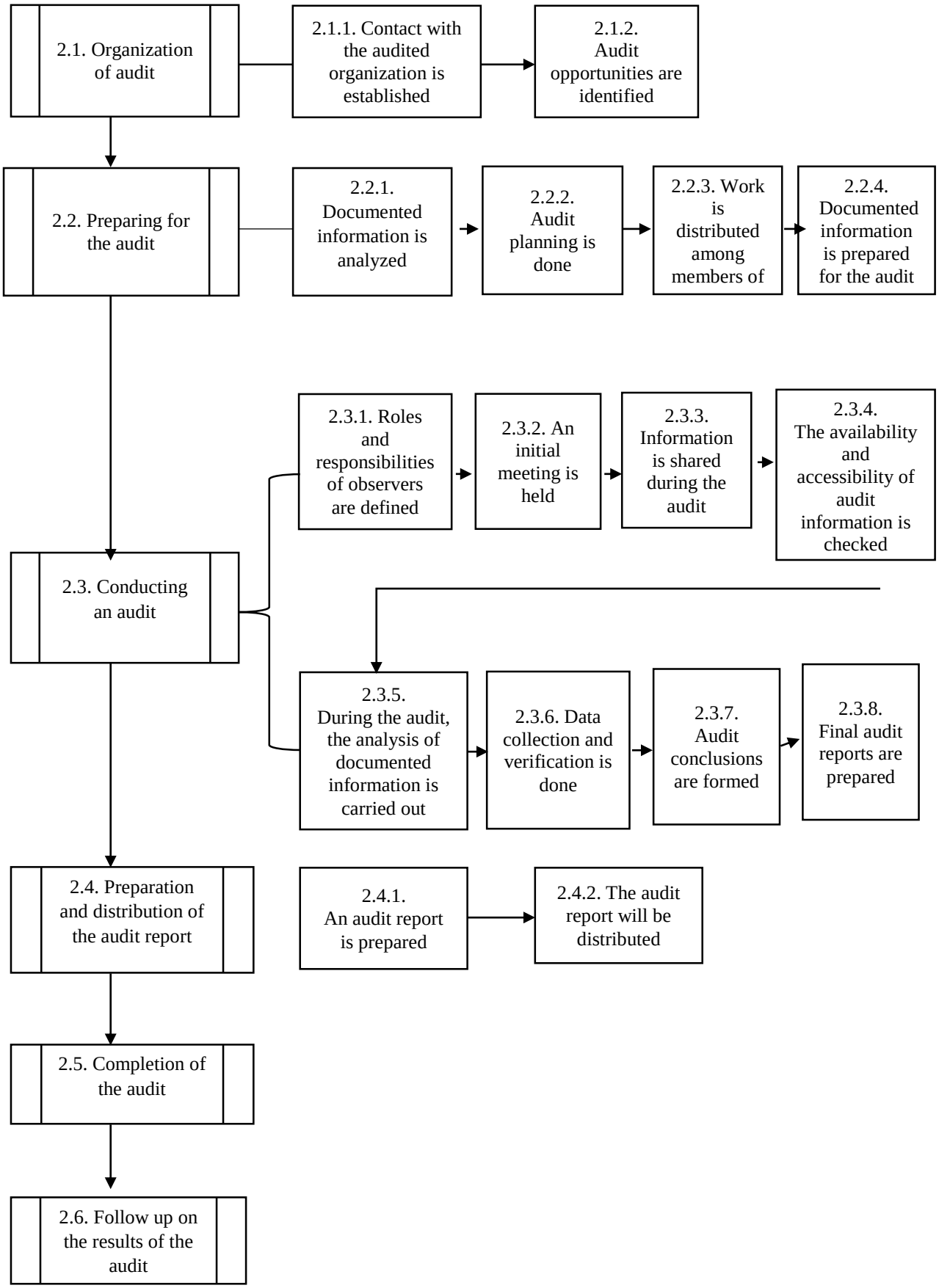

Figure 2. IT Cyber Security Audit Scheme

2.2.1 Documented information is analyzed

2.2.2 Audit planning is carried out

2.2.3 Work is distributed among members of the audit team

2.2.4 Documented information is prepared for the audit

2.3. Auditing.

2.3.1 Roles and responsibilities of observers are defined

2.3.2 An initial meeting is held

2.3.3 Information is shared during the audit

2.3.4 Availability and accessibility of audit information is checked

2.3.5 Analysis of documented information is carried out during the audit

2.3.6 Data collection and verification is performed

2.3.7 Audit conclusions are formed

2.3.8 Final stops on the audit are prepared

2.3.9 A final meeting will be held

2.4. Preparation and distribution of the audit report;

2.4.1. An audit report is prepared

2.4.2. The audit report will be distributed

2.5. Completion of the audit;

2.6. Further actions on audit results.

The proposed information model for auditing information systems can be presented in the form of such an algorithm.

The steps of the algorithm for conducting an IT cyber security audit are carried out in the following order and volume:

1. Deciding on the need to conduct an audit is the initial stage;
2. Then the preparation for conducting the audit begins;
3. In the next step, the contract is signed;
4. Then the audit team is formed;
5. Then information about the current state of IT is collected;
6. The initial data and documents received are analyzed and evaluated;

Figure 3. Description of the stages of conducting a cyber security audit

If the initial data and the analysis of the documents are consistent with the audit requirements, a plan for the implementation of audit work is prepared. If the conducted analysis does not meet the requirements, then the possibility of continuing the audit will be reconsidered;

1. If it is possible to continue the audit, then the identified shortcomings are quickly eliminated and repeated analysis of the received data and documents is carried out, otherwise the audit is not conducted and recommendations are immediately developed;

Figure 4 shows the flow chart of an IT cyber security audit, according to which the flow of the audit can be easily understood.

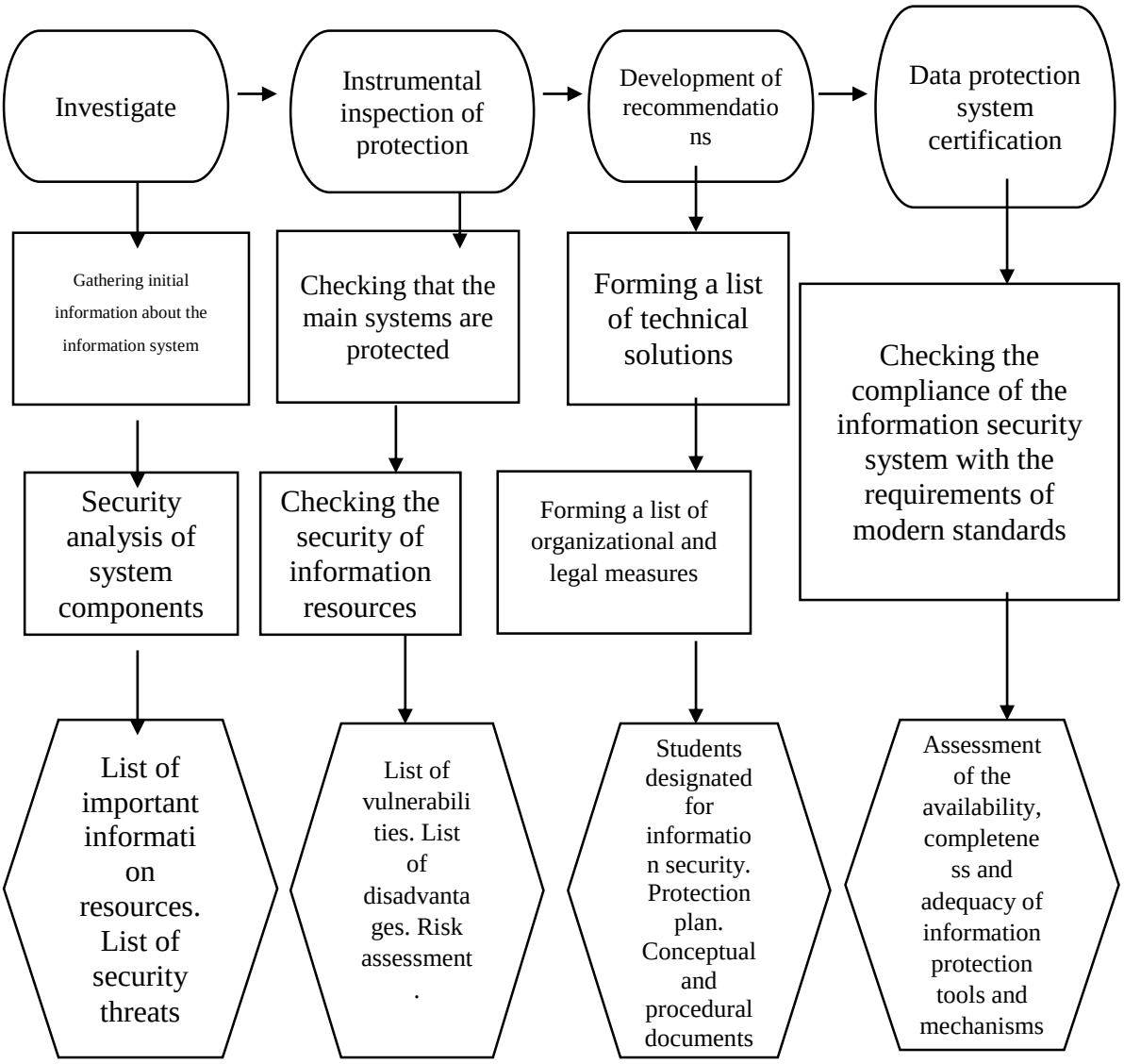

Figure 4. IT Cyber Security Audit Scheme

1. After preparing the audit work plan, the facility will be audited;

2. Then the compliance of the provided initial data with the actual IT working conditions is checked;

3. In the next step, the technological process of data processing and storage is studied, as well as information flows are analyzed;

4. Then the compliance of the preliminary data provided by the customer with the actual conditions of deployment, installation and use of the automated information system is carried out;

After that, a survey of the organization's employees is conducted, the correctness of determining the level and class of IT protection is assessed, the objects of computing equipment in the AAT are classified, the completeness and level of the development of organizational-distribution, project and application documents are assessed, the level of training of employees and the responsibility for the fulfillment of requirements for ensuring IT protection is evaluated.

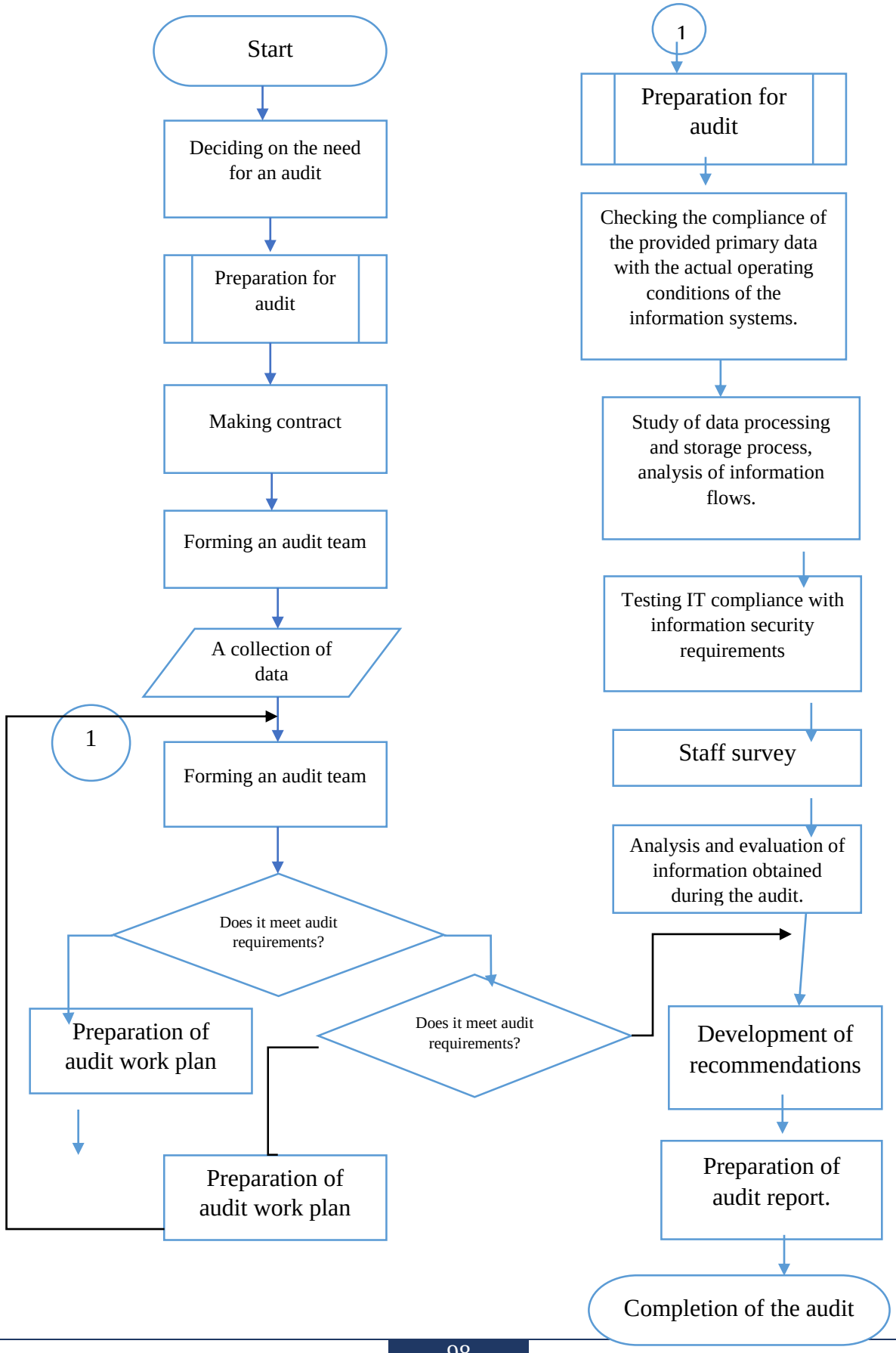
Start
Deciding on the need for an audit
Preparation for audit
Making contract
Forming an audit team
A collection of data
1
Forming an audit team
Does it meet audit requirements?
Preparation of audit work plan
Preparation of audit work plan
Does it meet audit requirements?
1
Preparation for audit
Checking the compliance of the provided primary data with the actual operating conditions of the information systems.
Study of data processing and storage process, analysis of information flows.
Testing IT compliance with information security requirements
Staff survey
Analysis and evaluation of information obtained during the audit.
Development of recommendations
Preparation of audit report.
Completion of the audit

Figure 5. IT cyber security audit algorithm

1. In the next step, the analysis and evaluation of the data obtained as part of the audit is carried out;

2. Next, recommendations are developed;

3. In the final step, an audit report is prepared with the conclusions of the audit team on IT compliance with information security requirements.

Development of recommendations for improvement of audit methods

There is a need to develop a simple information security audit system to ensure stability and security in order to minimize the demands on experts.

An audit mechanism should record all system activity that may be related to malicious attacks.

In addition to initially configuring the audit engine by selecting the events in the system that should be flagged, auditors also perform audit event analysis. This audit mechanism should be protected from unauthorized use by senior management. In this case, it is necessary to control the permissions to configure the audit mechanism, allowing only system auditors.

Audit means the analysis of collected data, which is carried out quickly, at the same time or periodically. The process of collecting and storing information about events that occur in the information system is called protocolization. Each service has its own set of possible events: external (caused by other services), internal (caused by its own service) and client (caused by users and administrators).

Ultimately, the following events can be distinguished:

1. Login may be successful or unsuccessful;

2. Sign out

3. Switching to a remote system;

4. Open, close, rename, delete, etc. operations on files containing functions;

5. Preferential right or mode of use, level of reliability of the user, etc. such as switching security attributes.

When describing the event, you should write the following necessary information:

1. Date and time of the incident;

2. Unique identifier of the user - the initiator of the action;

3. Type of event;

4. Action result;

5. Request source;

6. Names of objects involved, such as files to be opened or deleted;

7. Description of changes made to the security database, for example, a new comment on object security.

The terms "declaration" and "audit" are characterized by a relationship unlike other information security tools and technologies. While identification and authentication are the starting point of user accountability, logical access control serves to protect the confidentiality and integrity of access data. It should be noted that cryptographic methods are also used for protection.

One of the main tasks of auditing is to identify suspicious activity and provide information for automatic or manual response to the data.

Suspicious activity is understood as malicious behavior of a user or an information system component in accordance with the organization's predetermined security policy or illegal behavior according to accepted criteria.

Reconstruction of the sequence of events allows to determine the fate of the vulnerability in the protection of the organization's services, find the culprit of the illegal access to the system, assess the level of damage and return to normal and stable operation.

Therefore, it is necessary to study the proposed general framework, which defines the basic information about the duties and responsibilities of auditors in the field of safety, from the beginning of the work.

In conclusion, if an auditor or other user is suspected of attacking an information system, it is technically possible to record their actions, down to keystrokes and mouse movements. This provides not only the ability to investigate security mode violations, but also to roll back some changes.

REFERENCES

1. Лившиц И.И. Модели и методы аудита информационной безопасности интегрированных систем управления сложными промышленными объектами [текст]: диссертация на соискание ученой степени доктора технических наук: специальность 05.13.19 / И. И. Лившиц: СПб., 2018. – 210 с.
2. Скабцов Н. Аудит безопасности информационных систем. — СПб.: Питер, 2018. — 272 с.: ил. — (Серия «Библиотека программиста»).
3. Макарова Л.Ю., Штефан М.И., Ковина А.М. Основы аудита. Самоучитель. Учебник. — М.: Издательский дом Высшей школы экономики, 2018. — 408 с.
4. Гулак М.Л. Аудит информационной безопасности. Прикладная статистика: учебное пособие / М. Л. Гулак, М. Ю. Рытов, О. М. Голембиовская. – М.: Ай Пи Ар Медиа, 2020. – 121 с.
5. ГОСТ Р ИСО/МЭК 27007-2014. Информационная безопасность. Методы и средства обеспечения безопасности. Руководства по аудиту систем менеджмента ИБ. – М.: Стандартинформ, 2015. – 23 с.
6. Белоус А.И., Солодуха В.А. Основы кибербезопасности. Стандарты, концепции, методы и средства обеспечения. - М.: Техносфера, 2021. – 482 с.
7. Зефиров, С.Л. Оценка информационной безопасности объекта при проведении аудита информационной безопасности / С. Л. Зефиров, А. Ю. Щербакова // Информационные системы и технологии ИСТ-2020: Сборник материалов XXVI Международной научно-технической конференции, Нижний Новгород, 2020. – С. 517-522.
8. Постановление Президента Республики Узбекистан от 21.11.2018 г. N ПП-4024 "О мерах по совершенствованию системы контроля за внедрением информационных технологий и коммуникаций, организации их защиты"
9. Сагитова В.В. Модели и алгоритмы анализа информационных рисков при проведении аудита безопасности информационной системы персональных данных [текст]: диссертация на соискание ученой степени доктора технических наук: специальность 05.13.19 / В. В. Сагитова: УФА., 2019. – 229 с.