ACTIVITIES AND OUTPUTS OF THE EVALUATION PROCESS

Sultanov Kamoliddin Muxiddin O'g'li
Student of Tashkent University of Information Technologies
Named After Muhammad Al-Khwarizmi

Beknazarova Saida Safibullaevna
Doctor of Technical Sciences, Professor of Tashkent
University of Information Technologies Named After Muhammad Al-Khwarizmi

PURPOSE OF THE EVENT

Collection of evaluation certificates in compliance with the conditions for ensuring a reliable assessment of information security.

INTRODUCTION

An independent assessment of the information security can be carried out with the help of an internal and external audit of the information security. In [3], an information security audit is defined as a systematic, independent and documented process of obtaining evidence of an organization's activities to ensure information security, establishing the degree of fulfillment of information security criteria in the organization, as well as allowing the possibility of forming a professional audit judgment about the information security of the organization.

The necessary conditions for ensuring a reliable assessment of information security during the audit are:

- Use of a trusted audit process and compliance with the basic audit principles;
- Management of the IB audit program;
- Use of the most reliable sources of evaluation evidence;
- Determination of the sample size taking into account the specified reliability of the evaluation evidence;
- Consideration of factors affecting audit risk in order to reduce audit risk.

The basic principles of conducting an IB audit [5] include:

- independence of the IB audit.

The auditors (the evaluation group) are independent in their activities and are not responsible for the activities that are audited by the IB. Independence is the basis for impartiality in conducting an information security audit and objectivity in forming an opinion on the results of an information security audit;- completeness of the IB audit.

The IS audit should cover all areas of the IS audit that correspond to the evaluation objectives. In addition, the completeness of the information security audit is determined by the sufficiency of the requested and provided materials, documents and the level of their compliance with the assigned tasks. The completeness of the IB audit is a prerequisite for the formation of objective conclusions based on the results of the IB assessment; - assessment based on the evidence of the IB audit.

In case of a periodic IS audit, an assessment based on the IS audit evidence is the only way to obtain a repeatable conclusion based on the results of the IS audit, which increases the credibility of such a conclusion. For the repeatability of the conclusion, the IB audit certificates must be verifiable; - reliability of the IB audit certificates.

Appraisers should be confident in the reliability of the evidence of the IB assessment. The credibility of the documentary evidence of the IS assessment increases when their reliability is confirmed by a third party or the management of the organization. The credibility of the facts obtained during the survey of the employees of the evaluation object increases with the confirmation of these facts from various sources [1]. The credibility of the facts obtained by monitoring the activities in the field of information security of the object of assessment increases if they are obtained directly during the functioning of the procedures or processes being checked;

- Competence and ethical behavior.

Trust in the process and results of the IB assessment depends on the competence of those who conduct the IB audit and on the ethics of their behavior. Competence is based on the auditor's ability to apply knowledge and skills. Ethical behavior implies responsibility, integrity, the ability to keep a secret, impartiality [2].

Compliance with the principles of conducting an information security audit is a prerequisite for objective conclusions based on the results of the assessment.

The main methods of obtaining evaluation certificates should be:

- Verification and analysis of documents related to the object of evaluation;
- Monitoring of the processes of the evaluation object;
- Survey of employees of the evaluation facility and an independent (third) sides.

Along with manual methods of collecting information, the formation of audit certificates can be automatic or semi-automatic as a result of the use of some tool or the use of several tools.

When collecting data, appraisers should proceed from the fact that information security activities in the field of assessment are carried out in accordance with the criteria for assessing information security, if there is evidence of this. Appraisers should show a sufficient degree of professional skepticism regarding the collected evaluation evidence, taking into account the possibility of violations of information security.

Verification and analysis of documents allow the appraiser to obtain evaluation certificates that have the greatest completeness and ease of perception and use compared to other methods of obtaining audit certificates. However, these audit certificates have varying degrees of reliability depending on their nature and source, as well as on the effectiveness of control over the process of preparation and processing of submitted documents.

Evidence of the assessment of information security obtained as a result of verification and analysis of documents can be, for example:

- Availability of a document(s) with relevant content;
- Excerpts from the document (documents) confirming the implementation of information security activities, assigning responsibility and responsibilities to the employee (employees) for the implementation of information security activities;
- Excerpts from the document(s) containing descriptions of implemented ZM, information security processes.

Surveillance is the appraiser's monitoring of the procedures or processes for ensuring information security performed by other persons (including the personnel of the organization).

Information is considered reliable only if it is received directly at the time of functioning of the procedures or processes being checked.

Audit evidence obtained by monitoring activities may be, for example, records, facts or other information related to the results of automatic control by technical means recorded by appraisers during the observation.

An oral survey is conducted by appraisers among employees (owners of assets) approved by a representative of the object of evaluation to provide sources of evidence and evaluation evidence. The results of oral surveys should be made out in the form of a protocol or a brief summary, in which the surname, first name, patronymic of the appraiser who conducted the survey, last name, first name, patronymic of the person being interviewed, as well as their signatures must be indicated. Forms with lists of questions of interest can be prepared for conducting standard surveys. The results of the oral survey should be checked, since the interviewee can express his subjective opinion.

REFERENCES

1) ISO/IEC 27004, Information technology — Security techniques — Information security management — Measurement.
2) Gartner. The Price of Information Security. Strategic Analysis Report
3) Kurilo A.P., Zefirov S.L., Golovanov V.B., etc. Information security audit. - M.: Publishing group "BDC-press", 2006— - 304s.