

# **LP-A Methodology of Information and Communication Security Audit**

**Authors:**

**Krzysztof Liderman  
Adam E. Patkowski**

## **Table of contents**

List of terms and symbols

Introduction

Chapter 1 Audit team composition; responsibilities and qualifications of its members

Chapter 2 Tools of the audit team

- 2.1. Questionnaires
- 2.2. Editable document templates
- 2.3. Security scanners
- 2.4. Inventory scanners
- 2.5. Configuration scanners

Chapter 3 Audit processes

Chapter 4 Specification of audit documents

- 4.1. IPO tables
- 4.2. Consolidated specification of documents

Chapter 5 Data flow diagrams

Chapter 6 Best practices

- 6.1. Best practices applied on formal path
- 6.2. Best practices applied on technical path

Summary

## List of terms and symbols

### TERMS

**audit** – a procedure aimed at assessing the compliance of the audited object with a model (standard, procedure model or subjectively established value vector of certain features), conducted by an independent party (company, person or team). In the case of an information and communication audit, such independence should be maintained in relation to:

- 1) the organisation/team that builds the security system;
- 2) hardware and software vendors;
- 3) the audited organisation, in the sense that the audit team must not be composed of employees of the audit outsourcer organisation.

**auditor** – a member of the audit team who conducts research and analyses.

**qualifying auditor** – a member of the audit team who is authorised to formulate generalizing appraisals from the research conducted by the audit team; s/he is in particular authorised to issue final audit judgments as regards the conformity of the identified facts of the case with the general audit model .

**security** – the degree of reasonably justified (e.g. through risk analysis) trust that potential losses will not be sustained. (coll.) - not yielding to fear; peace; the confidence that nothing bad will happen.

**information and communication security** – the degree of justified trust (compare to e.g. ISO/IEC 15408) that potential loss resulting from undesired (accidentally or intentionally caused) disclosure, modification, destruction or making it impossible to process information stored or transmitted by means of information and communication systems, will not be incurred.

**sensitive information** – for a given entity, it includes all information which might be used against such an entity through its disclosure, making it unavailable or through its overt or hidden manipulation. This includes, in particular, all information which has to be protected as set forth in the relevant provisions of law in force (e.g. the *law on personal data protection*) and such information for which the obligation to protect it is not contained in any legal regulations, and which for particular organisations developing or processing such information is indicated by competent authorities, e.g. state protection services, internal security cells in a given organisation, the plenipotentiary for information security, etc.

**methodology** (French *métodique* derived from *méthode* "a method") 1. the accepted principles which specify the manner of completing a given type of work, research, etc.; the manner of proceeding. 2. *scientific*: in didactics – the principles of teaching a given subject, based on detailed specification of objectives, resources and methods of obtaining them. (*Słownik Wyrazów Obcych*” Wyd. Europa. 2001)

**vulnerability** – defects or gaps in physical structure, organisation, procedures, personnel, management, administration, hardware or software, which can be used for effecting damage in a computer system or user’s operations.

#### NOTES

1 – The mere presence of vulnerability does not cause loss. Vulnerability is only a condition or a set of conditions which make damage to the system or interference with the user’s operations through an attack possible

2 – if vulnerability corresponds to threat, risk exists.

(point 3.1.064 of PN-I-02000:1998)

**security measures** – physical measures (e.g. a fence), technical measures (e.g. an alarm system), human resources (e.g. a guard), software measures (e.g. anti-virus software) or organisational actions (e.g. training courses), used in order to counteract the exploitation of vulnerability resulting from threats. Security measures are frequently referred to in short as protections.

**threat** – potential violation of computer system protections.

*(point 3.1.115 of PN-I-02000:1998)*

**information and communication resources** – any physical resources (e.g. a safe box), technical resources (e.g. air-conditioning devices, computers), various forms of information resources (e.g. hard copy technical network documentation, the content of electronic databases), to which unauthorised access to or damage of which can result in compromising the confidentiality, integrity or accessibility of the information which is processed, stored or transferred in information and communication systems and networks.

## GRAPHIC SYMBOLS



a **process** symbol in DFD



a **terminator** symbol, that is an external element in relation to the processes described by means of DFD.



a **warehouse** symbol, that is an element which can store data (documents or other, depending on the modeled context, elements).



a symbol of data flow (flow of documents, information, etc.) between the elements of DFD.

### NOTE!

Graphic symbols of processes and warehouses indicated in DFD diagrams with a dashed line denote duplicated processes and warehouses, which means that these are the same processes and warehouses as the ones drawn with a solid line, and are only put on the diagram again in order to obtain better transparency (drawings of flows, which blur the diagram, are avoided).

## Introduction

The present document describes the LP-A methodology of audit in the field of information and communication. The methodology pertains to conducting an audit of information and communication system and networks (office, databases, etc.), in which the subject of protection is information. This methodology **is not applied** when conducting an audit in the field of widely-meant security of control systems and networks (industrial ones, to which the IEC 61508 Standard applies), in which these systems' environment is protected from the consequences of their improper operation.

The methodology presented below consists of:

- 1) organisation, scope of competences and qualifications of the audit team (chapter 1)
- 2) tools of the audit team (Chapter 2)
- 3) documents necessary for initiating the audit and developed during the audit (chapter 4)
- 4) a model in the form of DFD diagrams, describing the document development processes and their interrelations (Chapters 3 and 5)
- 5) a list of best practices, that is heuristic procedures, developed and verified in the course of the auditing practice of methodology creators (Chapter 6).

The elements of IT systems' structural method have been used for the presentation of processes and document flow during the audit. These elements include above all IPO (*Input–Process–Output*), DFD (*Data Flow Diagrams*), and the identification terms and symbols of processes, flows and warehouses used for them (see “*List of terms and symbols*” at the beginning of the present study).

According to the definition presented at the beginning of this document, an audit is a procedure aimed at assessing the compliance of the audited object with the model. For the purpose of the present methodology, the ISO/IEC 27001 Standard has been accepted as the model. Such an assumption results from the professional experience of the creators of the present methodology – at present, virtually all orders for work in the field of information and communication security refer to this standard and no changes in this respect are envisaged. This belief is reflected in the recommendation of the European Union dated 28.02.2002 “*on a common approach and specific actions in the area of network and information security*” (2002/C 43/02) pointing to specific standards in the field of information and communication security: ISO/IEC 15408 in the field of certification and ISO/IEC 17799 (the precursor of ISO/IEC 27001) in the field of best practices. Nevertheless, there is nothing against entering another norm or standard in IPO tables instead of the ISO/IEC 27001 Standard, provided one has properly prepared tools for it, mainly in respect of materials, that is, audit questionnaires.

It needs to be pointed out that an information and communication security audit which is compliant with the methodology presented herein does not consist only of substantiation based on documentation analyses, surveys and site visits, which assess the degree of compliance of information and communication security management in the audited object (e.g. institution) with the model. Such documenting takes place in the course of realisation of the so-called *formal path* (see Chapter 3). However, the comparison with recommendations is conducted with a certain violation of equality of individual verifications. Some of them, regarded as particularly important, are verified in greater detail than others; although standard procedure means verification, in particular cases, the actions taken should be treated as research. This category includes testing the effectiveness of technical and IT protections as well as a system analysis of protections. **The characteristic feature of LP-A methodology is the realisation** within the so-called *technical path* (see Chapter 3) of **tests** of physical and

technical protection systems and information and communication systems and networks in use in the audited object. These tests are conducted with the use of specialised tools and are complemented with penetration tests, primarily heuristic ones.

The effect of taking on such a mode of action is:

- 1) the possibility of detecting particularly dangerous vulnerabilities and submitting to the Employer, through the auditors, a specification of vulnerabilities “for immediate removal” (the separate question remains as to who is to remove the identified vulnerabilities – due to formal considerations, this should not be done by the audit team);
- 2) completing and improving the depth and the quality of assessments generated as part of the formal path;
- 3) submitting to the Employer a full picture (both technical and organisational) of the state of protections of his networks and systems, which usually constitutes the basis for further actions of the Employer in the field of information and communication security.

Based on the information included in the present description, the following can be done:

- 1) assessment of the complexity of processes which are part of the audit;
- 2) tracing the interrelations between the documents generated in the audit process;
- 3) selecting the members of the Audit Team, taking into account the required competences (qualifications and rights) of the team members;
- 4) assessing, based on the interdependencies between the processes (and the members of the Team), the possibility of running the audit tasks simultaneously;
- 5) preparing the audit realisation schedule (having accounted for specific terms and conditions resulting from the agreement with the Employer);
- 6) estimating the costs of audit completion (also having accounted for terms and conditions of the agreement).

Chapter 6 presents the best practices, which are procedural methods which belong to the know-how category, in most cases heuristic ones, developed and verified in the course of the auditing practice of methodology creators. Although these practices have been listed above as methodology elements, it has to be noted that they are closely related to a specific team of people (their qualifications, experience, ethics, etc.). For this reason, the content of chapter 6 should be treated rather as a guideline, and not as a “strict” instruction – each team of auditors will probably develop their own set of best practices. However, the authors of the presented methodology hope that the set presented in Chapter 6 will be assessed positively and will be included in the repertoire of actions of other audit teams.

## Chapter 1

### Members of the audit team, their qualifications and competences

Among the key factors that decide the reliability of the conducted audit are the qualifications and the methods of work of the audit team members. This chapter contains information on the composition and qualifications of the team. The work methods, resulting from the implemented and verified methodology, are described in Chapter 3.

The audit team is composed of two parts:

- fixed part
- variable part (“on the phone”).

#### I. Fixed team

##### 1. **Qualifying auditors** – two persons (symbols: AK\_1 and AK\_2)

Requirements:

- a) technical university education
- b) at least several years of professional experience in the field of computer systems, in particular in the field of information and communication security
- c) at least several years of practice in conducting audits in the field of information and communication security
- d) didactic experience and negotiation skills
- e) authorisations of the relevant National Security Authorities to access to non-public information (e.g. in Poland – as provided for in the law on “*access to non-public information*”).

The main tasks of the qualifying auditors include:

- realisation of tasks at the audit preparatory stage (see Chapter 3)
- realisation of formal path tasks from the audit realisation stage, in cooperation with the specialists referred to in points 2 and 3 of this chapter
- supervision over the completion of technical path tasks
- preparing the final report from technical analyses
- submitting the specification of identified "Vulnerabilities for immediate removal" to the Employer
- preparing the final document from the information and communication security audit at the Employer’s Institution.

Qualifying auditors sign the post-audit documents as the guarantors of the information included therein.

##### 2. **Physical and Technical Protection Specialist** (symbol: SF-T)

Requirements:

- a) university education
- b) at least several years of professional experience in the field of computer systems, in particular in the field of information and communication security
- c) practice in conducting audits in the field of information and communication security

- d) 2<sup>nd</sup> degree technical protection employee license
- e) authorisations of the relevant National Security Authorities to access to non-public information (e.g. in Poland – as provided for in the law on “access to non-public information”).

The tasks of the physical and technical protection specialist include:

- cooperation with qualifying auditors in the completion of formal path tasks of the audit realisation stage;
- realisation of points 4.2.1 and 4.2.2 (see Chapter 3) of the technical path of the audit realisation stage;
- preparing the report from the analysis of physical and technical protection systems

### 3. **Privacy Protection and Electromagnetic Radiation Specialist** (symbol: SA-PU)

Requirements:

- a) technical university education
- b) at least several years of professional experience in the field of computer systems and in the field of installation and detection of specialised technology devices
- c) practice in conducting audits in the field of information and communication security
- d) authorisations of the relevant National Security Authorities to access to non-public information (e.g. in Poland – as provided for in the law on “*access to non-public information*”).

The basic duties of the Privacy Protection and Electromagnetic Radiation Specialist include:

- cooperation with qualifying auditors in the completion of formal path tasks from the audit realisation stage (see Chapter 3);
- realisation of points 4.2.3 and 4.2.4 (see Chapter 3) of the technical path of the audit realisation stage;
- preparing the report from the technical analysis.

### 4. **Network Devices and Computer Networks Specialist** (symbol: SUS-SK)

Requirements:

- a) technical university education
- b) at least several years of professional experience in the field of computer systems and in the field of organisation and operation of networks and design of network devices
- c) practice in conducting audits in the field of information and communication security
- d) authorisations of the relevant National Security Authorities to access to non-public information (e.g. in Poland – as provided for in the law on “*access to non-public information*”).

The duties of the Network Devices and Computer Networks Specialist include:

- cooperation with qualifying auditors (see Chapter 3) in the completion of formal path tasks from the audit realisation stage;
- supervision over the work of branch experts (see Chapter 3);
- participation in the development of technical analysis reports

5. **Back office personnel** (symbol: PP)

Back office personnel, occupied with e.g. copying, binding, etc. of relevant documents, has to hold authorisations of the relevant National Security Authorities to access to non-public information (e.g. in Poland – as provided for in the law on “*access to non-public information*”) if working on such documents. In certain cases (e.g. in case of interviewers), such personnel needs to hold the appropriate authorisations of the Employer to perform certain tasks on the site of his Institution.

**II. Variable team** (symbol: ED)

The variable team consists of members who are selected as needed by branch experts. Branch experts are selected by qualifying auditors to meet the needs of a particular audit, depending on systems (hardware and software), which are particularly numerous or particularly important for the audited computer system (e.g. Solaris, Windows XP, Novell, etc.) and particular personnel requirements, e.g. related to holding authorisations to access non-public information.

## Chapter 2

### Tools of the Audit Team

The tools of the audit team include:

1. Questionnaires prepared based on the instructions included in the standard (e.g. ISO/IEC 27001).
2. Editable document templates.
3. Automated tools (programs), primarily:
  - Security scanners
  - Inventory scanners
  - Configuration scanners

#### 2.1. Questionnaires

Questionnaires prepared based i.e. on the ISO/IEC 17799 Standard, contain 913 in-depth questions divided into the following ten thematic groups (the numbering, which starts from 3, is compliant with the numbering of the ISO/IEC 17799 Standard):

3. Security policy
4. Security organisation
5. Asset classification and control
6. Personal safety
7. Physical and environmental security
8. System and network management
9. System access control
10. System development and maintenance
11. Business Continuity Management
12. Compliance

The questionnaire, filled in and verified based on interviews and inspections, is the basis for judgments as regards the degree of fulfilment of the requirements of 139 audit points resulting from the instructions of the ISO/IEC 17799 Standard. In case of application of the ISO/IEC 27001 Standard, the number of questionnaire questions and verification points is slightly different.

#### 2.2. Editable document templates

For most of the documents generated in the course of an audit, templates have been developed, regarding at least their editing, and in some cases setting forth the distribution of subject matter content. However, there are no objections as to the development of the company's own documentation models (if assuming LP-A as the company's internal audit

standard in the field of information and communication security), stemming from the organisational culture of the business.

## 2.3. Security scanners

A scanner is any entity (e.g. a device or a program), which reviews a certain set of objects in a certain order. A security scanner is a program or a computer system controlled by such a program, which scans the computers which are part of a certain given set, and which checks for the presence of vulnerabilities. In the general model, the object checked by the security scanner is the Cartesian product of the set of computers subject to the test and the set of vulnerabilities. For each element (vulnerability on the computer), the value of the presence function is determined (vulnerability: present/not present).

The outcome of the security scanner operation is a report, which in its basic form contains a list of vulnerabilities identified for each computer (present on a given computer), and for each vulnerability it specifies: an identifier according to recognised classification (e.g. *bugtraq*), description, degree of threat and removal method.

A security scanner is a set of procedures (in some cases programs or scripts), which carry out real attack attempts. Each successful attack is recorded and information about it is included in the final report, generated by the scanner. The use of a security scanner without agreeing it with the computer system administrator is in Poland treated as a violation of Article 267<sup>1</sup> of the Penal Code (the “acquired information” being the information on the state of protections).

Security scanners<sup>2</sup> contain sets of vulnerability signatures and attack patterns. Such data should be updated along with changes in the state of the art in this field. The subscription of this data is included in the offer of commercial security scanners.

## 2.4. Inventory scanners

Inventory scanners are a group distinguished by the authors, due to their specific application: identifying and preparing specifications of all services present in the scanned computers. Usually, for this purpose, the extended ports scanner<sup>3</sup> is used as an inventory scanner, or any of the older versions of security scanners<sup>4</sup> – the selection criterion is the ease of generating the appropriate reports.

---

<sup>1</sup> Article 267 of the Penal Code

§1. Any person, who without authorisation obtains information which has not been designed for him, through opening a letter, connecting to a conduit serving to transmit information or through breaking electronic, magnetic or other particular protections, is subject to fine, restriction of freedom or imprisonment of up to 2 years.

<sup>2</sup> In the year 2006, these were, e.g.: nessus (open source), NetRecon (Symantec), Retina (eEye) or Internet Security Scanner (ISS).

<sup>3</sup> In the year 2006, these were, e.g.: nmap.

<sup>4</sup> In the year 2006, an example of such a scanner, effective mainly in large office Windows networks, is *Languard Network Security Scanner* version 3.3 (the developer, GFI Software Ltd., already offers version 7.0 of this product).

## 2.5. Configuration scanners

A configuration scanner is a program used for automatic remote testing of configuration settings (including so-called protection rules) of each of the computers within a given set, and generating appropriate reports. This testing consists in accessing configuration files (e.g. MS Windows system registry) of the tested computer and comparing the records in such files to a model which has been regarded as valid by the scanner's producer. Moreover, configuration scanners check the records in configuration files related to patches installed, distributed by the producers – the absence of such patches is regarded as a vulnerability. The drawback of configuration scanners is the necessity of remote access to the tested computers with administrator access rights, which is normal in Windows domain networks, but does not comply with security principles in most networks which are organised differently.

The most popular<sup>5</sup> program of this class is MBSA (*Microsoft Baseline Security Analyzer*, designed for Windows systems, produced by Shavlik Technologies for Microsoft Corp.).

---

<sup>5</sup> In 2006

## Chapter 3

### Audit processes

Further in this chapter, we describe in general and with comments the audit processes assigned to individual stages of audit, and include information (table 3.1) about who from the Audit Team is responsible for each process and who oversees each process.

#### I. Audit preparatory stage

1. Preliminary meeting with the Employer's representatives:
  - 1.1. Presentation of members of the audit team, submission of documents (including, if needed, security certifications), determining the scope of authorisations of auditors to collect and access the Employer's information, **setting the date of issuing the relevant regulations, giving the auditors formal permission to operate in the Employer's jurisdiction (!)**. The issuance of such regulations is necessary in order to begin the realisation stage of the audit – in practice, this stage can be realised only **after** they are announced at the Employer's institution.
  - 1.2. Appointing the chief consultant (contact person) and, if needed, a Team of Consultants on the part of the Employer. The Chief Consultant (and members of the Team of Consultants) has to be authorised to issue opinions and make binding statements on behalf of the Employer
  - 1.3. Appointing persons, on the part of the Employer, with competences in individual thematic stages of the audit. Auditors can formulate judgments based on information collected from all available sources, in particular from each employee of the Employer. However, the Employer should indicate employees who are particularly competent in providing information on the "state of affairs." Contrary to consultants (see point 1.1), who have the right to interpret, take a position and express will on behalf of the Employer, the indicated employees only provide information, reliable according to their knowledge and in the best will of each of them.
  - 1.4. Agreeing on the principles of communication between the Employer's personnel and the audit team (in particular, the responsibility for delays and postponing the date of completion of works):
    - the principles of planning the consultancy and document authorisation by the consultants
    - the principles of collecting the information among the Employer's employees
    - the principles of conducting audit works – performing the tasks for the auditors by the Employer's employees (auditors' rights to independent actions, the Employer's personnel's rights to supervision, auditors' rights to request assistance)
  - 1.5. Setting the schedule of audit works.

2. Running (as required) a seminar which shapes the awareness of the management staff of the Employer's institution in the field of audits and information and communication security. Practice shows that such a seminar allows the Employer's management staff and the employees who cooperate with the auditors to formulate their views on the scope of audit works and unify the understanding of terms and notions related to information and communication security in a wide sense.

## **II. Audit realisation stage**

### **3. Formal path**

As part of actions taken on this procedural path, auditors test the management of information and communication security at the Employer's Institution as regards compliance with the audit model specified in the agreement (e.g. as regards compliance with BS 7799 guidelines, the ISO/IEC 17799 Standard or the ISO/IEC 27001 Standard—for simplicity's sake, further in the methodology description, it has been assumed that this audit model is the ISO/IEC 17799 Standard).

The basic processes of the formal path are:

- 3.1. Collecting from the Employer and analysing documentation that establishes the legal order in the studied institution – subordination, responsibility and rights – in the field of information and communication security (statutes, regulations, employment cards, contracts, etc.).
- 3.2. Collecting from the Employer and analysing documentation that establishes the relations between the Employer and third parties (contracts and other documents), in particular:
  - documentation transferring the responsibility for information and communication resources of the Employer onto other legal entities, including outsourcing and insurance contracts as well as data archiving contracts;
  - documentation establishing the Employer's responsibility for third party resources (all contracts);
  - agreements between the Employer and other entities, permitting the access of third party employees to the Employer's resources or resources entrusted to the Employer (verification of ensuring the conditions for due diligence in the field of information and communication security).
- 3.3. Submitting the thematic audit questionnaires for completion by persons (who are competent in the individual thematic scopes of the audit) who are appointed on the part of the Employer and identified in point 1.3.
- 3.4. Local inspections and interviews at the Employer's seat or at locations for some reason important to the Employer, carried out by auditors in order to formulate a preliminary opinion on the practical management of information and communication security at the Employer's Institution.
- 3.5. Collecting the completed questionnaires (submitted according to point 3.3) and analysing them.
- 3.6. Meeting, as required, the persons who completed the questionnaires, in order to clarify any doubts, correct errors and insufficiencies, compare the findings with the results of technical tests and repeated (if required) local inspections and interviews.
- 3.7. Final analysis and study of the questionnaires.

- 3.8. Preparing the final report which contains the opinion on conformity with the ISO/IEC 17799 Standard (or other standard constituting the basis for audit).

#### 4. Technical path

As part of tasks performed on this procedural path, at the first stage, auditors analyse the technical documentation of information and communication systems and networks as well as physical and technical protection systems (including the fire protection and power supply systems). The aim of the analysis is:

- to discover insufficiencies in the documentation;
- to prepare penetration tests and research using automated tools;
- to prepare (if required) electromagnetic radiation measurements;
- to reveal conceptual errors in the network and system structure;
- to prepare the data for the final report from the tests carried out in the technical path.

At the second stage of actions of auditors and branch experts, the necessary (or contractually agreed) measurements and tests of network and systems are carried out. The important outcome of the activities carried out as part of the technical path is the detection of vulnerabilities “for immediate removal”, that is, such vulnerabilities whose removal will considerably reduce the risk of loss of confidentiality, integrity or availability of the information processed, stored and transmitted by the Employer.

The basic processes of the technical path are:

- 4.1. Analysing the submitted technical documentation of networks and systems (information, communication and technical) of the Employer.
- 4.2. Testing the status of physical and technical protection:
  - 4.2.1. Review of physical and technical protections, including fire protections.
  - 4.2.2. Review of the power supply system supplying power to the Employer’s devices and systems.
  - 4.2.3. Electromagnetic radiation measurement (if required)<sup>6</sup>.
  - 4.2.4. Searching for wiretapping devices and checking the Personal Protection Equipment (if required).
  - 4.2.5. Preparing the preliminary report from the tests of physical and technical protection systems.
- 4.3. Studying the information and communication protection status:
  - 4.3.1. Carrying out randomised configuration tests of selected computers in the Employer’s networks and systems.
  - 4.3.2. Testing vulnerability using automated tools<sup>7</sup> in selected (or, depending on specific arrangements, in all) networks and systems of the Employer.
  - 4.3.3. Testing configuration settings using automated tools in selected (or, depending on specific arrangements, in all) networks and systems of the Employer.

---

<sup>6</sup> In Poland, in case of carrying out an audit regarding compliance with the requirements of the law on “protection of non-public information” in the scope of information classified as a state secret, this is an obligatory point of the audit schedule.

<sup>7</sup> Works carried out in close cooperation with the Employer’s technical administrators.

- 4.3.4. Testing application patches using automated tools in selected (or, depending on specific arrangements, in all) networks and systems of the Employer.
- 4.3.5. Analysing the results of tests obtained in points 4.3.1–4.3.4, and preparing the specification of “Vulnerabilities for immediate removal.”
- 4.3.6. Performing supplementary penetration tests.
- 4.3.7. Updating the specification of “Vulnerabilities for immediate removal.”
- 4.3.8. Stocktaking, if required, using automated inventory tools, of the components of the Employer’s networks and systems.
- 4.4. Submitting (upon written acknowledgement of receipt) the specification of identified "Vulnerabilities for immediate removal" to the Employer.
- 4.5. Preparing the final report from technical analyses.

### **III. Audit reporting stage**

5. Preparing the final document from the information and communication security audit at the Employer’s Institution.
6. Submitting to the Employer the set of audit documents (reports, printouts from scanning tools, etc.) – delivering the study entitled “Information and communication security audit at (name of the Employer’s institution).” Besides the formal delivery of documents, this point may also contain the presentation of the results of the audit to the Employer by the qualifying auditor.

**Table 3.1** Scopes of responsibilities and supervision over the audit processes

<b>Process no.</b>	<b>Short description of the process</b>	<b>Person responsible</b>	<b>Supervision</b>
1.1	preliminary arrangements	AK_1	AK_2
1.2	appointing the consultant(s)	AK_1	AK_2
1.3	appointing the informants	AK_1	AK_2
1.4	agreeing on the principles of communication	AK_1	AK_2
1.5	setting the schedule	AK_1	AK_2
2	Seminar	AK_2	AK_1
3.1	collecting and analysing the documentation on the legal order	AK_2	AK_1
3.2	collecting and analysing the documentation on relations with third parties	AK_2	AK_1
3.3	submitting the questionnaires to be filled in	AK_2	AK_1
3.4	local inspections and interviews	AK_1	AK_2
3.5	collecting and analysing the questionnaires	AK_2	AK_1
3.6	completing the questionnaires	AK_2	AK_1
3.7	studying the questionnaires	AK_2	AK_1
3.8	preparing the report on compliance with the ISO/IEC 17799 Standard	AK_2	AK_1
4.1	analysis of technical documentation	SF-T, SA-PU, SUS-SK	AK_1
4.2.1	review of physical and technical protections	SF-T	AK_1
4.2.2	review of power supply system	SF-T	AK_1
4.2.3	measurement of electromagnetic radiation	SA-PU	AK_1
4.2.4	searching for wiretapping	SA-PU	AK_1
4.2.5	analysis of the Team's internal notes	AK_1	AK_2
4.3.1	random configuration tests	SUS-SK or ED	AK_1
4.3.2	vulnerability testing (automated)	SUS-SK or ED	AK_1
4.3.3	configuration testing (automated)	SUS-SK or ED	AK_1
4.3.4	patch testing (automated)	SUS-SK or ED	AK_1
4.3.5	analysis of results of information and communication network tests	AK_1	AK_2
4.3.6	manual penetration tests	ED	SUS-SK
4.3.7	updating the vulnerability specification	AK_1	AK_2
4.3.8	stocktaking of resources (automated)	SUS-SK or ED	AK_1
4.4	submitting the information on vulnerabilities	AK_1	AK_2
4.5	preparing a report on technical tests	AK_1	AK_2
5	preparing the final audit document	AK_1	AK_2
6	submitting the results of audit to the Employer	AK_1	AK_2

## Chapter 4

### Specification of audit documents

In this chapter, documents related to the audit process are specified, using the IPO (*Input–Process–Output*) method. At the end of the chapter, in tables 4.1 and 4.2, are the documents necessary for carrying out audit works and documents generated during the audit.

#### 4.1. IPO tables

##### Explanations for IPO tables:

1. The (\*) symbol by the process number denotes that such a process is decomposed into sub-processes.
2. Documents denoted in the tables as a “note” are divided into two types:
  - 1) Team’s memos - authorised records, copies delivered to the Employer
  - 2) Team’s internal notes – unauthorised records, no copy sent to the Employer.
3. A dashed line indicates borders of tables with optional processes (that is, carried out upon the specific contractual request of the Employer).
4. Bolded text indicates basic output documents from the audit, submitted to the Employer.

Input	<ul style="list-style-type: none"> <li>• Team’s authorisation documents</li> <li>• RFQ or Terms of Reference</li> <li>• agreement</li> </ul>
Process no.	1
Process	Preliminary meeting with the Employer’s representatives
Output	<ul style="list-style-type: none"> <li>• scope of authorizations</li> <li>• audit regulations</li> <li>• the regulation on the seminar (optional)</li> <li>• schedule</li> <li>• authorised memo 1 of the Team</li> </ul>

Input	<ul style="list-style-type: none"> <li>• Team's authorisation documents</li> <li>• RFQ or Terms of Reference</li> <li>• agreement</li> </ul>
Process no.	1.1
Process	presentation of members of the audit team, submitting the documents (security certifications), determining the scope of authorisations of auditors to collect and access the Employer's information, agreeing on the date of issuing the relevant regulations, giving the auditors formal permission to operate under the Employer's jurisdiction.
Output	<ul style="list-style-type: none"> <li>• scope of authorizations</li> <li>• audit regulations</li> <li>• the regulation on the seminar (optional)</li> </ul>

Input	scope of authorizations
Process no.	1.2
Process	appointing the chief consultant (contact person) on the part of the Employer – the representative who has the right to interpret, take a position and express will on behalf of the Employer
Output	authorised memo 1 of the Team

Input	<ul style="list-style-type: none"> <li>• scope of authorizations</li> <li>• agreement</li> </ul>
Process no.	1.3
Process	appointing persons, on the part of the Employer, with competences in individual thematic stages of the audit.
Output	authorised memo 1 of the Team

Input	<ul style="list-style-type: none"> <li>• scope of authorizations</li> <li>• agreement</li> </ul>
Process no.	1.4
Process	agreeing on the principles of communication between the personnel of the Employer and the audit team (in particular, the responsibility for delays and postponing the date of completion of works)
Output	authorised memo 1 of the Team

Input	<ul style="list-style-type: none"> <li>• scope of authorizations</li> <li>• authorised memo 1 of the Team</li> <li>• RFQ or Terms of Reference</li> <li>• the offer</li> <li>• agreement</li> </ul>
Process no.	1.5
Process	setting the schedule
Output	schedule

Input	the Employer's regulation on the place and the date of the seminar
Process no.	2 (optional)
Process	Running (as required) a seminar which forms the awareness of the management staff of the Employer's institution in the field of audit and information and communication security.
Output	<b>seminar materials</b>

Input	<ul style="list-style-type: none"> <li>• scope of authorizations</li> <li>• statute</li> <li>• regulations</li> <li>• individual obligations of employees (employee cards, lists of duties, etc.)</li> <li>• contracts transferring the responsibility for the Employer's information and communication resources onto third party entities (outsourcing and insurance contracts)</li> <li>• documentation establishing the Employer's responsibility for third party resources (all contracts)</li> <li>• contracts between the Employer and other entities, permitting third party employees' access to the Employer's resources or resources entrusted to him</li> <li>• audit questionnaires</li> <li>• audit regulations</li> <li>• final report from analyses and technical tests</li> </ul>
Process no.	3 (*)
Process	testing compliance with the ISO/IEC 17799 Standard (formal path)
Output	<b>final report on compliance with the ISO/IEC 17799 Standard</b>

Input	<ul style="list-style-type: none"> <li>• statute</li> <li>• regulations</li> <li>• internal security regulations</li> <li>• employee cards</li> <li>• contracts</li> </ul>
Process no.	3.1
Process	collecting from the Employer and analysing the documentation establishing the legal order in the studied institution – subordination, responsibility and rights – in the field of information and communication security
Output	written opinion on organisational documentation

Input	<ul style="list-style-type: none"> <li>• contracts transferring the responsibility for the Employer’s information and communication resources onto third party entities (outsourcing and insurance contracts)</li> <li>• documentation establishing the Employer’s responsibility for third party resources (all contracts)</li> <li>• contracts between the Employer and other entities, permitting third party employees’ access to the Employer's resources or resources entrusted to him</li> </ul>
Process no.	3.2
Process	collecting from the Employer and analysing the documentation establishing relations between the Employer and third parties (verification of ensuring the conditions for due diligence in the field of information and communication security)
Output	written opinion on organisational documentation

Input	<ul style="list-style-type: none"> <li>• audit questionnaires</li> <li>• scope of authorizations</li> </ul>
Process no.	3.3
Process	Submitting the thematic audit questionnaires for completion by persons (who are competent in the individual thematic scopes of the audit) appointed on the part of the Employer and identified in process 1.3.
Output	a note (specification with signatures of the persons who take the questionnaires) on the questionnaires issued, with the return date indicated

Input	scope of authorizations
Process no.	3.4
Process	local inspections and interviews at the Employer’s seat (or at the locations specified in the agreement)
Output	internal notes of the Team from local inspections and interviews (interviews authorised if required)

Input	<ul style="list-style-type: none"> <li>• list of persons to whom audit questionnaires have been issued</li> <li>• completed questionnaires</li> <li>• Team’s internal notes from local inspections and interviews</li> <li>• final report from analyses and technical tests</li> </ul>
Process no.	3.5
Process	collection of the questionnaires submitted in the process and their analysis
Output	list of items to be completed (“asked”) – internal note of the Team

Input	<ul style="list-style-type: none"> <li>• scope of authorizations</li> <li>• completed questionnaires</li> <li>• list of items to be completed (“asked”) – internal note of the Team</li> </ul>
Process no.	3.6
Process	meeting, as required, the persons who completed the questionnaires, in order to clarify any doubts, correct errors and insufficiencies, compare the findings with the results of technical tests and repeat (if required) local inspections and interviews.
Output	completed questionnaires

Input	<ul style="list-style-type: none"> <li>• completed questionnaires</li> <li>• notes from inspections and interviews</li> <li>• opinion on the documentation (output documents of processes 3.2, 3.2, 4.1)</li> <li>• final report from analyses and technical tests</li> </ul>
Process no.	3.7
Process	studying the questionnaires
Output	prepared questionnaire

Input	<ul style="list-style-type: none"> <li>• notes from inspections and interviews</li> <li>• opinion on the documentation (output documents of processes 3.2, 3.2, 4.1)</li> <li>• prepared questionnaire</li> <li>• final report from analyses and technical tests</li> </ul>
Process no.	3.8
Process	preparing the final report on compliance with the ISO/IEC 17799 Standard
Output	<b>final report on compliance with the ISO/IEC 17799 Standard</b>

Input	<ul style="list-style-type: none"> <li>• scope of authorizations</li> <li>• technical documentation of networks and systems (information, communication and technical) of the Employer</li> </ul>
Process no.	4 (*)
Process	testing the physical and technical systems as well as information and communication systems of the Employer (technical path)
Output	<b>final report from analyses and technical tests</b>

Input	technical documentation of networks and systems (information, communication and technical) of the Employer
Process no.	4.1
Process	analysis of the submitted technical documentation of networks and systems (information, communication and technical) of the Employer
Output	written opinion on organisational documentation

Input	technical documentation of physical and technical protection systems
Process no.	4.2 (*)
Process	testing the status of physical and technical protection
Output	<ul style="list-style-type: none"> <li>• report from the analysis of physical and technical protection systems</li> <li>• measurement results</li> </ul>

Input	technical documentation of physical and technical protection systems
Process no.	4.2.1
Process	review of physical and technical protections, including fire protections.
Output	internal note of the Team from the review of physical, technical and fire protection measures

Input	technical documentation of physical and technical protection systems
Process no.	4.2.2
Process	review of the power supply system supplying power to the Employer's devices and systems.
Output	internal note of the Team from the review of the power supply system

Input	technical documentation of physical and technical protection systems
Process no.	4.2.3
Process	measurement of electromagnetic radiation (optional)
Output	<ul style="list-style-type: none"> <li>internal note of the Team from zoning of buildings and premises</li> <li>results of the electromagnetic radiation measurements</li> </ul>

Input	technical documentation of physical and technical protection systems
Process no.	4.2.4
Process	searching for wiretapping devices and checking the Personal Protection Equipment (if required)
Output	internal note of the Team from the search for wiretapping devices and check of the Personal Protection Equipment

Input	<ul style="list-style-type: none"> <li>internal note of the Team from the search for wiretapping devices and check of the Personal Protection Equipment</li> <li>internal note of the Team from zoning of buildings and premises</li> <li>measurement results</li> <li>internal note of the Team from the review of the power supply system</li> <li>internal note of the Team from the review of physical, technical and fire protection measures</li> </ul>
Process no.	4.2.5
Process	analysis of internal notes of the Team
Output	report from the analysis of physical and technical protection systems

Input	technical documentation of information and communication networks and systems
Process no.	4.3 (*)
Process	studying the information and communication protection status
Output	<ul style="list-style-type: none"> <li>report from technical tests of information and communication networks and systems of the Employer</li> <li><b>specification of “Vulnerabilities for immediate removal”</b></li> <li><b>inventory record</b> (optional)</li> </ul>

Input	technical documentation of information and communication networks and systems
Process no.	4.3.1
Process	carrying out randomised configuration tests of selected computers in the Employer’s networks and systems
Output	internal note of the Team on the results of randomised configuration tests

<b>Input</b>	technical documentation of information and communication networks and systems
<b>Process no.</b>	4.3.2
<b>Process</b>	testing configuration settings using automated tools in selected (or, depending on specific arrangements, in all) networks and systems of the Employer
<b>Output</b>	internal note of the Team on the results of the conducted automated vulnerability tests + reports generated by the tools

<b>Input</b>	technical documentation of information and communication networks and systems
<b>Process no.</b>	4.3.3
<b>Process</b>	testing configuration settings using automated tools in selected (or, depending on specific arrangements, in all) networks and systems of the Employer
<b>Output</b>	internal note of the Team on the results of the conducted automated configuration tests + reports generated by the tools

<b>Input</b>	technical documentation of information and communication networks and systems
<b>Process no.</b>	4.3.4
<b>Process</b>	testing application patches using automated tools in selected (or, depending on specific arrangements, in all) networks and systems of the Employer
<b>Output</b>	internal note of the Team on the results of the conducted automated application patches tests + reports generated by the tools

<b>Input</b>	<ul style="list-style-type: none"> <li>• internal note of the Team on the results of randomised configuration tests</li> <li>• internal note of the Team on the results of automated application patches tests</li> <li>• internal note of the Team on the results of automated configuration tests</li> <li>• internal note of the Team on the results of automated vulnerability tests</li> <li>• reports generated by these tools</li> </ul>
<b>Process no.</b>	4.3.5
<b>Process</b>	analysis of the results obtained from tests of information and communication systems and networks
<b>Output</b>	<ul style="list-style-type: none"> <li>• instructions for the completion of supplementary heuristic penetration tests</li> <li>• preliminary specification of “Vulnerabilities for immediate removal”</li> <li>• a report from technical tests of information and communication networks and systems of the Employer</li> </ul>

Input	<ul style="list-style-type: none"> <li>instructions for the completion of supplementary heuristic penetration tests</li> <li>technical documentation of networks and systems</li> </ul>
Process no.	4.3.6
Process	performing supplementary heuristic penetration tests
Output	report from penetration tests

Input	<ul style="list-style-type: none"> <li>results of penetration tests</li> <li>preliminary specification of “Vulnerabilities for immediate removal”</li> </ul>
Process no.	4.3.7
Process	updating the specification of “Vulnerabilities for immediate removal”
Output	<b>specification of “Vulnerabilities for immediate removal”</b>

Input	technical documentation of networks and systems
Process no.	4.3.8 (optional)
Process	stocktaking, if required, using automated inventory tools, of the components of the Employer’s networks and systems
Output	the inventory record made using automated inventory tools

Input	completed specification of “Vulnerabilities for immediate removal”
Process no.	4.4
Process	submitting the specification of identified "Vulnerabilities for immediate removal" to the Employer
Output	confirmation of receipt of the specification of "Vulnerabilities for immediate removal" by the Employer

Input	<ul style="list-style-type: none"> <li>written opinion on organisational documentation</li> <li>report from technical tests of physical and technical protection systems</li> <li>report from technical tests of information and communication systems</li> <li>specification of “Vulnerabilities for immediate removal”</li> </ul>
Process no.	4.5
Process	preparing the final report from technical analyses
Output	<b>final report from analyses and technical tests</b>

Input	<ul style="list-style-type: none"> <li>• <b>final report from analyses and technical tests</b></li> <li>• <b>final report on compliance with the ISO/IEC 17799 Standard</b></li> </ul>
Process no.	5
Process	preparing the final document from the information and communication security audit at the Employer's Institution
Output	<b>final audit document</b>

Input	<b>final audit document</b>
Process no.	6
Process	submitting to the Employer the set of audit documents (reports, printouts from scanning tools, etc.) - acceptance of audit results
Output	confirmations of the receipt of the study entitled "Information and communication security audit at ( <i>name of the Employer's institution</i> )"

## 4.2. Consolidated specification of documents

**Table: 4.1. List of documents necessary for carrying out audit works**

No.	Document name	Delivered by:
1	agreement	Employer/Auditors
2	RFQ or Terms of Reference	Employer/Auditors
3	Audit Team's authorisation documents	Auditors
4	audit questionnaires	Auditors
5	technical documentation of physical and technical protection systems of the Employer	Employer
6	technical documentation of information and communication networks and systems of the Employer	Employer
7	Statutes of the Employer's institution	Employer
8	regulations in force in the Employer's institution	Employer
9	security regulations in force	Employer
10	individual obligations of employees (employee cards, lists of duties, etc.)	Employer
11	documentation transferring the responsibility for the Employer's information and communication resources onto third party entities (outsourcing and insurance contracts)	Employer
12	documentation establishing the Employer's responsibility for third party resources (all contracts)	Employer
13	contracts between the Employer and other entities, permitting third party employees' access to the Employer's resources or resources entrusted to him	Employer

### NOTE

The description Employer/Auditors in the column "Delivered by:" means that this is the preparatory document for carrying out audit works, certified copies of which are possessed by both the parties.

**Table: 4.2. List of documents produced in the audit process**

<b>No.</b>	<b>Document name</b>	<b>Document status</b>	<b>Produced by</b>
1	authorised memo 1 of the Team	internal	Aud./Empl.
2	scope of authorizations	official/initiating	Employer
3	audit regulations	official/initiating	Employer
4	schedule of audit works	official	Aud./Empl.
5	<i>seminar regulation</i>	official	Employer
6	<i>seminar materials</i>	official/delivery	Auditors
7	written opinion on the documentation establishing legal order in the institution and establishing the relationship between the Employer and third parties	official	Auditors
8	a note (specification with signatures of the persons who take the questionnaires) on the questionnaires issued	official	Auditors
9	internal notes of the Team from local inspections and interviews (interviews authorised if required)	internal	Auditors
10	completed questionnaires	internal	Aud./Empl.
11	list of items to be completed (“asked”) – internal note of the Team	internal	Auditors
12	completed questionnaires	internal	Auditors
13	prepared questionnaire	internal	Aud./Empl.
14	written opinion on organisational documentation	official	Auditors
15	internal note of the Team from the review of physical, technical and fire protection measures	internal	Auditors
16	internal note of the Team from the review of the power supply system	internal	Auditors
17	<i>internal note of the Team from zoning of buildings and premises</i>	internal	Auditors
18	<i>results of the electromagnetic radiation measurements</i>	internal	Auditors
19	<i>internal note of the Team from the search for wiretapping devices and check of the Personal Protection Equipment</i>	internal	Auditors
20	the report from the test of physical and technical protection systems	official	Auditors
21	internal note of the Team on the results of randomised configuration tests	internal	Auditors
22	internal note of the Team on the results of automated vulnerability tests	internal	Auditors
23	internal note of the Team on the results of automated configuration tests	internal	Auditors
24	internal note of the Team on the results of automated application patch tests	internal	Auditors

25	instructions for the completion of supplementary manual penetration tests	internal	Auditors
26	preliminary specification of “Vulnerabilities for immediate removal”	internal	Auditors
27	a report from technical tests of information and communication networks and systems of the Employer	internal	Auditors
28	results of manual penetration tests	internal	Auditors
29	specification of “Vulnerabilities for immediate removal”	official/delivery	Auditors
30	confirmation of receipt of the specification of "Vulnerabilities for immediate removal" by the Employer	official	Aud./Empl.
31	<i>the inventory record made using automated inventory tools</i>	official/delivery	Auditors
32	selected reports generated by the tools	official	Auditors
33	<b>final report from analyses and technical tests</b>	official/final	Auditors
34	<b>final report from the audit for compliance with the recommendations of the BS 7799 Standard or the ISO/IEC 17799 Standard</b>	official/final	Auditors
35	<b>final audit document</b>	official/final	Auditors
36	<b>confirmations of the receipt of the study entitled “Information and communication security audit at (name of the Employer’s institution)”</b>	official/final	Aud./Empl.

## NOTES

- Names of the documents in *italics* denote that these are the documents produced upon specific request of the Employer (as the output of optional processes in IPO tables).
- The description Aud./Empl. in the column “Produced by” denote that such a document is produced as a result of mutual arrangements between the auditors and the authorised representatives of the Employer, authorised by both the parties.
- Names of documents in **bold** denote final (settlement) audit documents.
- The status “Official/delivery” denotes that such a document is submitted to the Employer in the course of audit works.
- The status “Official/initiating” denotes that **such a document is necessary in order to begin the audit realisation stage** – it is the legal basis for all actions of the auditors at the site of the Employer’s Institution.
- The status “Official” denotes that the given document is the basis for preparing final audit documents or is entirely included in such documents.

## Chapter 5

### Data Flow Diagrams

Based on the diagrams included further in this chapter, the following can be done:

- 1) assessment of the complexity of processes which are part of the audit;
- 2) tracing the interrelations between the documents generated in the audit process;
- 3) assessing, based on the interdependencies between the processes and the members of the Team, the possibility of running the audit tasks simultaneously.

The presented diagrams are helpful in setting the schedule of audit works for a particular Employer. They make it possible to make him aware of the complexity of the undertaking and of the degree of involvement in the undertaking required from him (documents submitted, necessary regulations, consulting and training, resources made available, etc.).

The diagram (and the methodology as a whole) considerably supports the valuation of audit works for the Employer. It has to be noted that in the case of an audit carried out at an Institution with territorially distributed Branches and Representative Offices (or similar organisational units), the presented realisation stage processes will be duplicated. In case the Audit Team has sufficient human resources and the proper tools, if the particular contract requires, it is possible to run the audit's realisation stage works simultaneously (e.g. running the tests of information and communication networks and systems at the same time in all the Branches using automated tools).

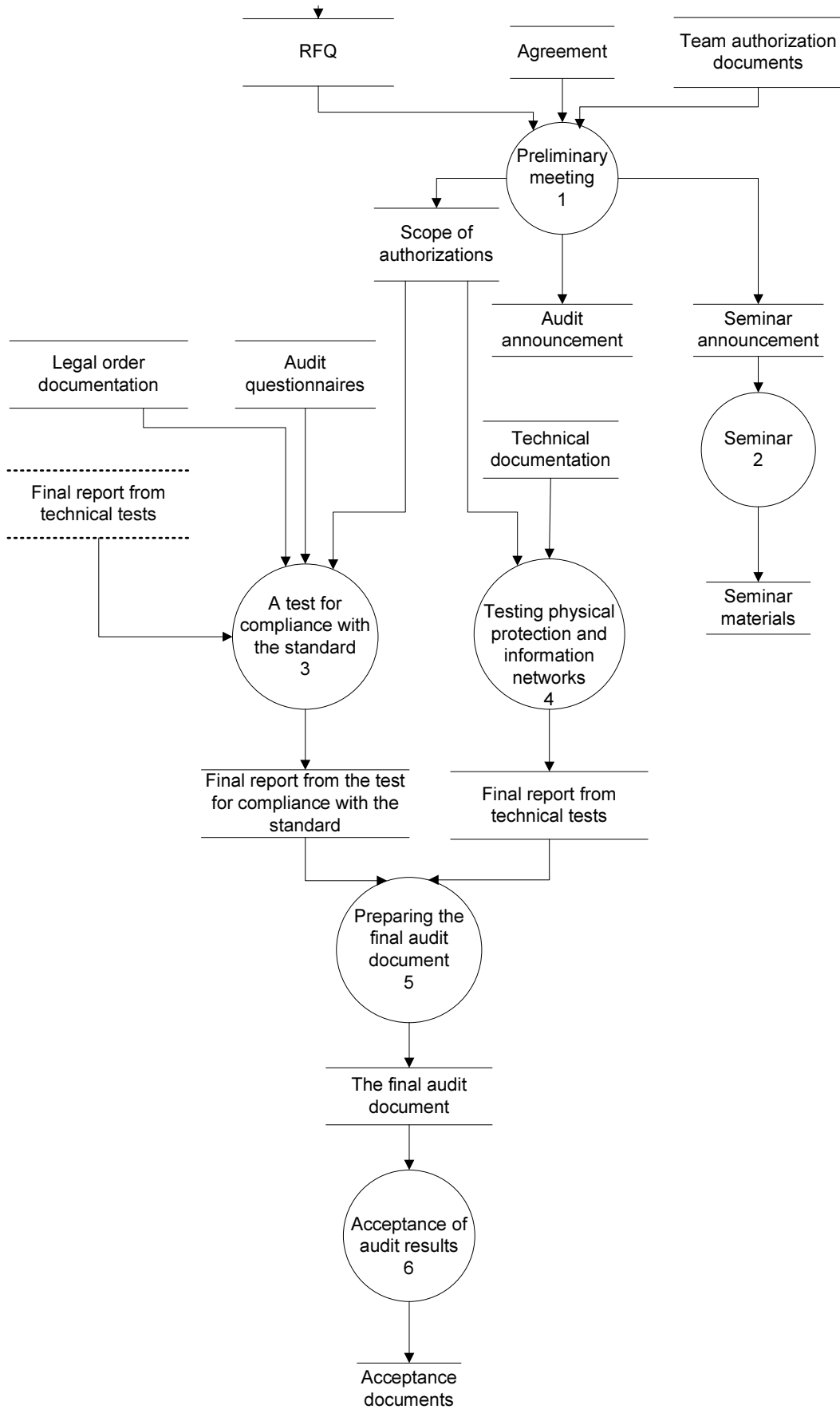
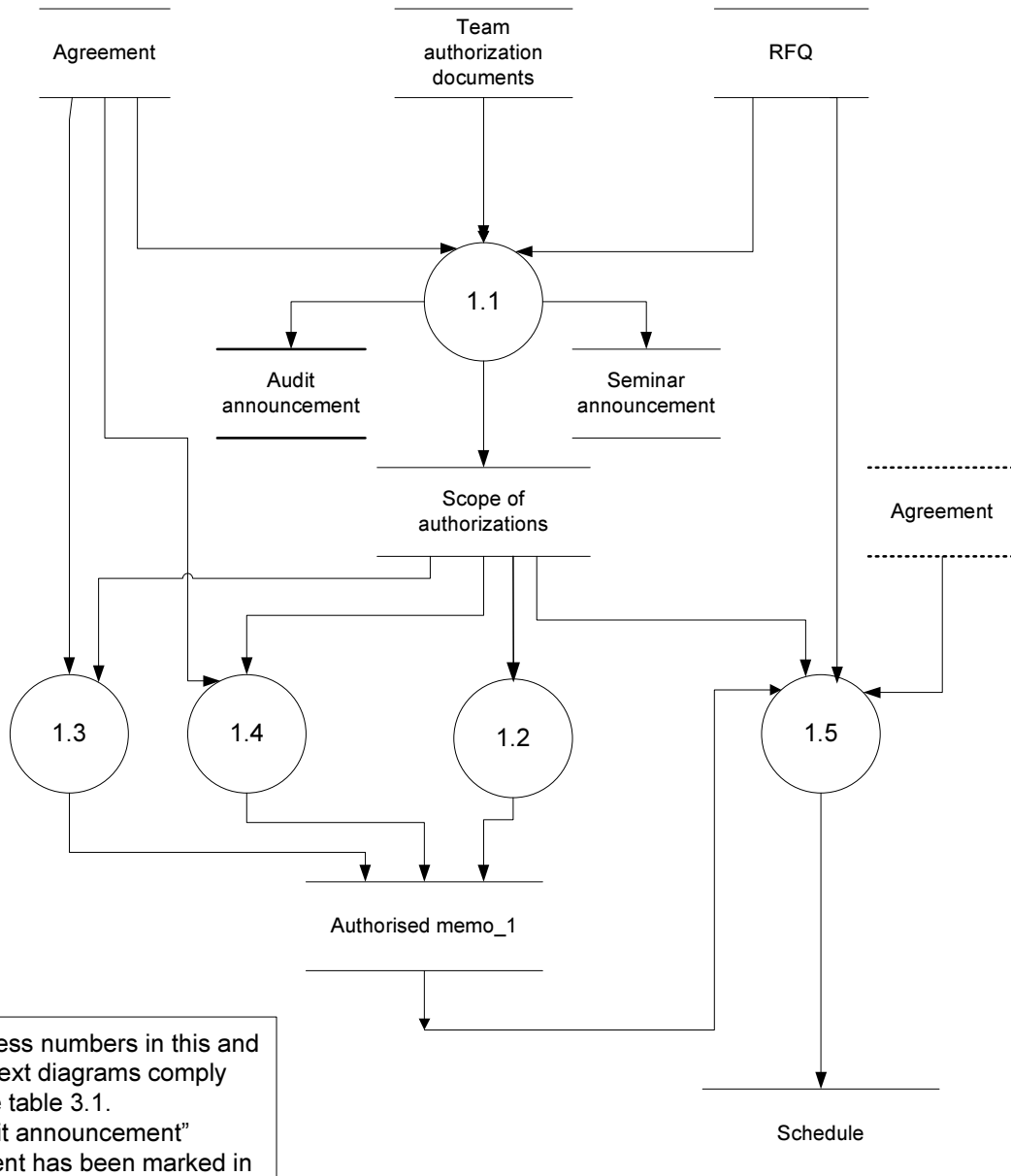


Diagram 1: DFD\_1 of the audit process – general outline



1. Process numbers in this and in the next diagrams comply with the table 3.1.  
 2. "Audit announcement" document has been marked in the diagram in bold, in order to underline its importance in the audit realisation.

Diagram 2: DFD\_2 – process no. 1.

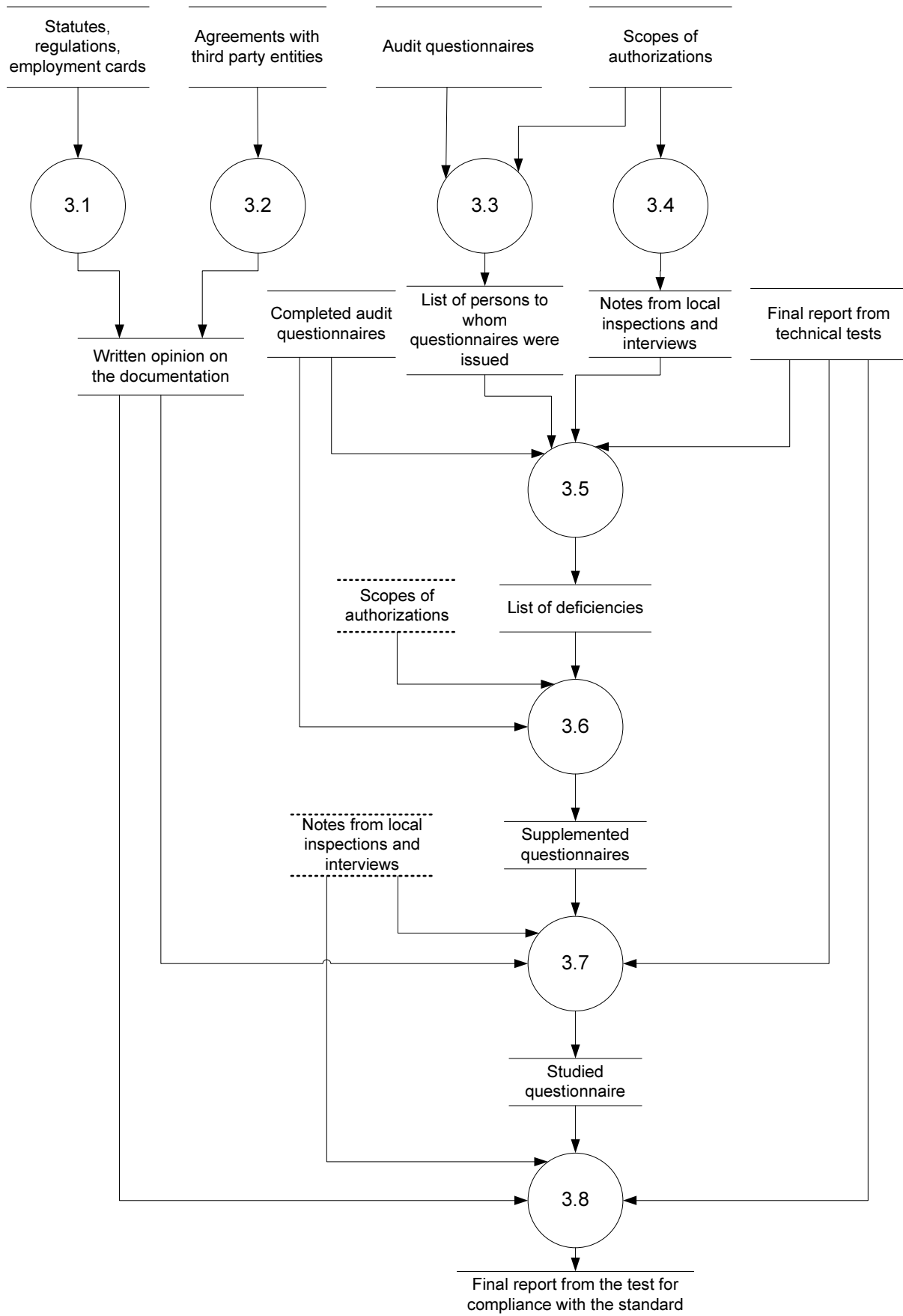


Diagram 3: DFD\_2 – process no. 3

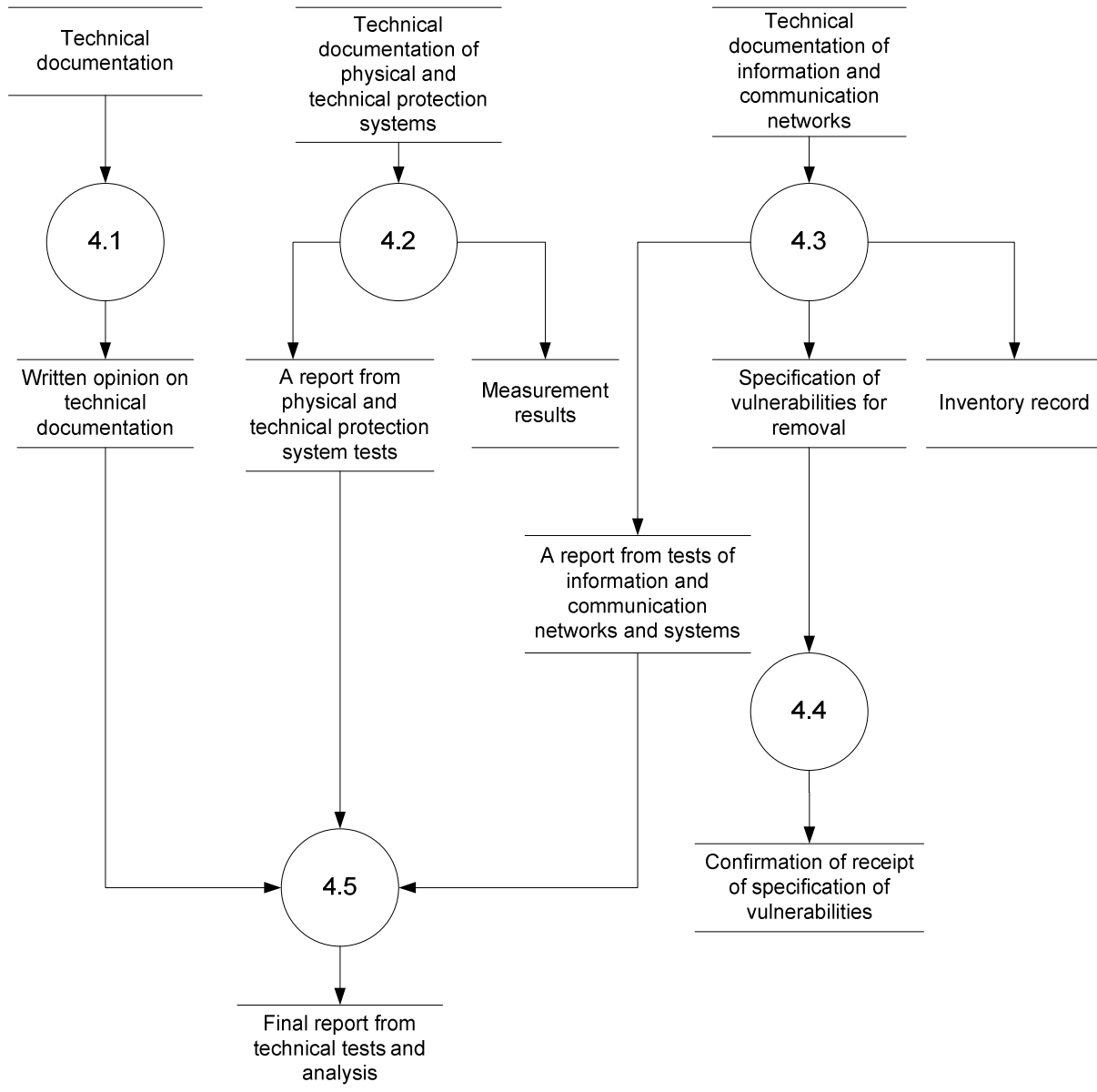


Diagram 4: DFD\_2 - process no 4

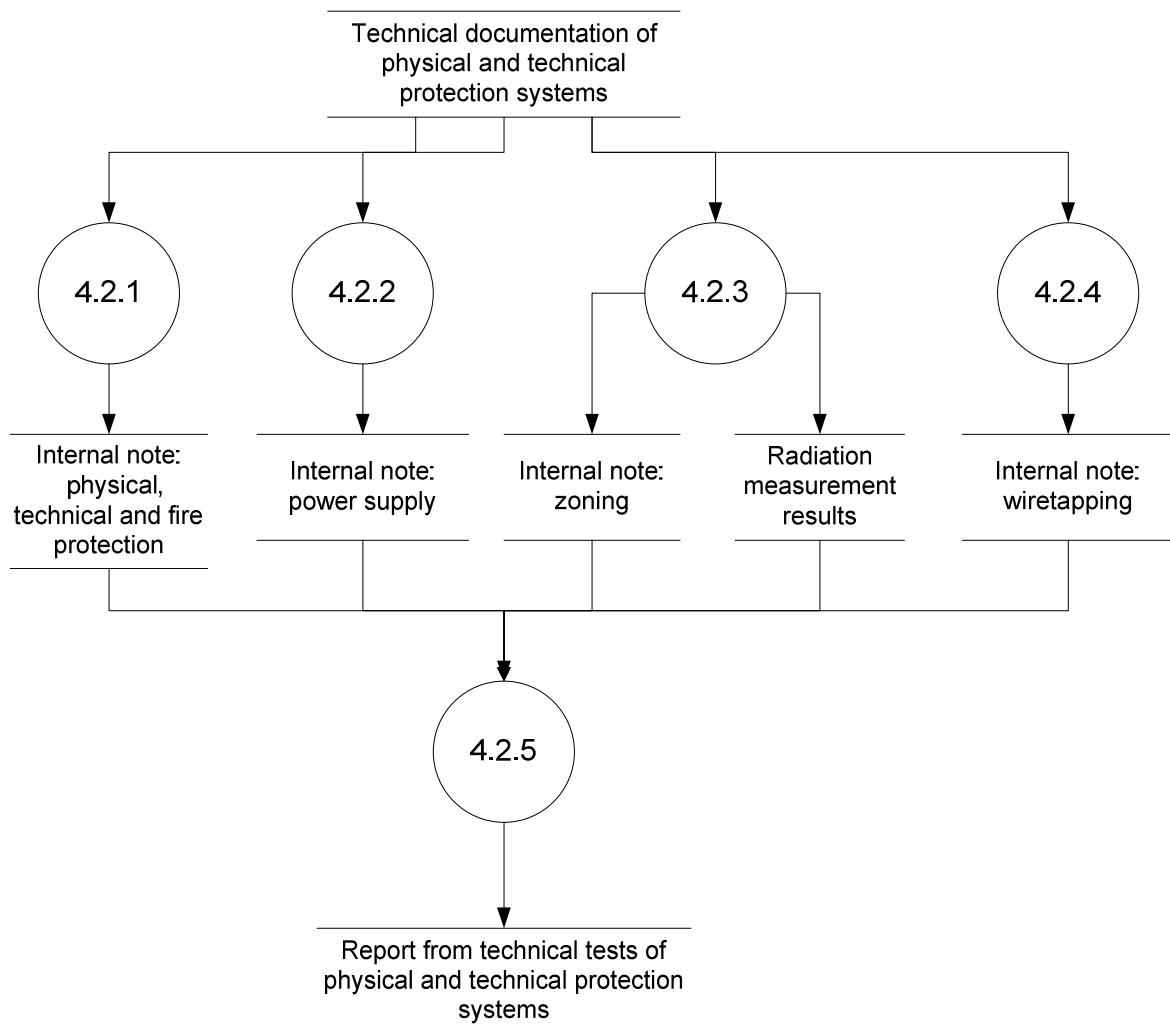


Diagram 5: DFD\_3 - process no. 4.2

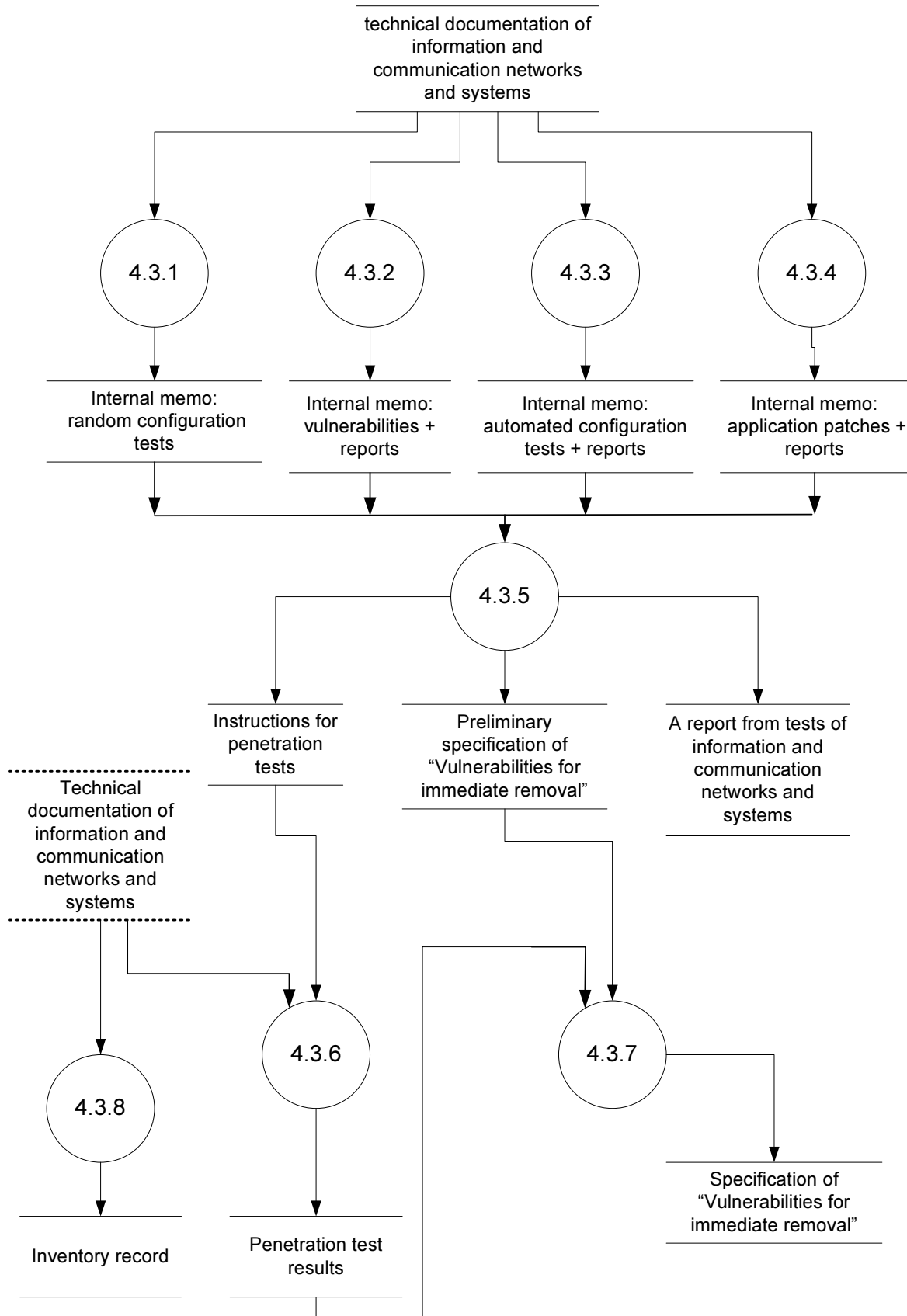


Diagram 6: DFD\_3 - process no. 4.3

## Chapter 6

### Best Practices

The present chapter contains the record of best practices, which are heuristic procedural methods which belong to the know-how category, developed and verified in the course of the auditing practice of methodology creators.

The two primary best practices are:

1. The team of auditors does not disclose any information related to the audit or acquired as a result of the audit without the consent of the Employer; in particular, the team of auditors does not include the name of the Employer's Institution in their letters of reference.
2. Customer focus – in the preparatory stage, the customer's real expectations are discussed (they might not be clearly set forth in the agreement), which makes it possible to focus on appropriate things at the realisation stage, e.g. in point 12 ("Compliance") of the ISO/IEC 17799 Standard, an in-depth analysis of compliance with the formal requirements in Poland as set forth in the law "*on personal data protection*" is possible.

#### 6.1. Best practices applied on the formal path

1. Each discussion, local inspection, etc. is always carried out by two members of the Audit Team.
2. An internal note from each discussion and local inspection is prepared, which can be authorised, if required, by the other party (in the Team's documents, the internal notes subject to authorisation are referred to as memos).

#### 6.2. Best practices applied on the technical path

1. Internal training of the Team – the specialist for networks and network devices (a member of the audit team) presents to the audit team the general model of information flow in the network or networks, including the packets' distribution zones and the installed separating mechanisms.
2. All the invasive operations in the Employer's systems are realised by the authorised employees of the Employer following auditors' instructions. Auditors do not assume the responsibilities of the competent employees of the Employer in any respect, even if they are permitted to act as operators, in order to speed up the works. In case of following these principles strictly, during the tests, the auditors will not physically touch any of the devices at all.
3. All the reviews (e.g. configuration of workstations) are performed by members of the audit team at all times assisted by a representative of the Employer (e.g. workstation administrator) and following his/her permission.

4. In case of discovering particularly dangerous vulnerabilities in the course of technical tests, the Employer is informed of such vulnerabilities **immediately** upon their discovery, without waiting for the completion of all the works connected with the audit. Such a course of action lets the Employer take immediate actions aimed at protecting (against exploitation of the existing and discovered vulnerabilities) the information processed, stored and transmitted in his information and communication systems and networks.

5. The principles of testing the configuration of workstations.

Servers, workstations and network devices are usually divided into three categories:

- **category I:** computers-bearers of sensitive information, as well as devices and connections whose functional degrading would mean compromising sensitive information;
- **category II:** computers and concentrators on which sensitive information might appear;
- **category III:** computers and other devices on which sensitive information is not processed or stored.

Configuration testing usually includes all the workstations and devices in category I and 2-5% of workstations and devices in category II. The choice of workstations for randomised tests should be performed based on rational premises – it would be most reasonable to select such a sub-set of workstations which would include all the workstations representative for various classes of the remaining computers included in category II.

## Summary

The described LP-A methodology can, in the opinion of its authors, support the management staff of companies and institutions which are interested in assessing the information and communication security status of computer systems and networks in making sound decisions as early as at the stage of RFQs and agreement drafts. In addition, teams of auditors that use this methodology can more precisely estimate the expenditures for carrying out an audit and plan the necessary undertakings. For instance, the description of LP-A methodology contains a list of 13 groups of documents which are necessary for conducting the audit works, a list of 36 documents produced in the audit process, and the interrelations between these documents.

Of considerable importance may also be the fact that if both the interested parties (the Employer and the Contractor) know the LP-A methodology, they use uniform terminology and have a uniform terminology basis for discussions and making concrete decisions.