TLP:CLEAR

PREMIER MINISTRE

Liberté
Égalité
Fraternité

Prime Minister

French National Cyber Security Agency

Cyber security audit service providers

Requirements baseline

Version 2.2 of 1 August 2024

Courtesy translation

TABLE OF CONTENTS

I. Introduction

I.1. Overview

I.1.1. Context

Information systems are changing, opening up more and more to the outside world and facing new threats. To protect themselves, organisations need to take a risk management approach to securing their information systems in a way that is appropriate and proportionate.

Cyber security audit service providers (PASSI) make it possible to:

- assess an information system's level of compliance with security requirements (rules, good practices, guides, baselines, standards, etc.);
- assess the security level of an information system;
- propose security measures to correct non-compliance and/or vulnerabilities identified during the audit.

The audit report drawn up by the cyber security audit service provider can be used particularly as part of the security accreditation of an information system.

I.1.2. Purpose of the document

This document constitutes the requirements baseline applicable to a cyber security audit service provider (PASSI), hereinafter referred to as "the service provider".

Its purpose is to qualify a service provider in accordance with the procedures described in section III.

It provides the client of an audit service with guarantees about the competence of the service provider and its staff, about the service provider's ability to perform a service that complies with the requirements of this baseline and to protect sensitive information and media to which it has access during the service.

It can also be used as best practice apart from any legal, regulatory or contractual requirements.

It does not replace the application of the legislation and regulations in force, in particular with regard to the protection of sensitive information (1) and classified information (2) or the obligations of service providers in their capacity as professionals, in particular their duty to advise their clients.

I.1.3. Document structure

Section I gives an introduction to this baseline.

Section II describes the activities covered by this baseline.

Section III describes the qualification procedures for a service provider.

Section IV describes the requirements applicable to the service provider.

Section V describes the requirements applicable to the service provider's staff.

Section VI describes the requirements applicable to the service.

Appendix 1 gives the bibliography.

Appendix 2 describes the knowledge, skills and tasks of the service provider's staff.

Appendix 3 provides recommendations for clients before, during and after the service.

I.2. Document identification

This baseline is called "Cyber security audit service providers – Requirements baseline". It can be identified by its name, version number and date of update.

I.3. Acronyms and definitions

I.3.1. Acronyms

The acronyms used in this baseline are:

ANSSI	French National Cyber Security Agency
PACS	Security support and consultancy service provider
PASSI	Cyber security audit service provider

I.3.2. Definitions

The definitions used in this baseline are as follows, based in part on the standard (3):

Audit – a systematic, independent and documented process for obtaining audit evidence and evaluating it objectively to determine the extent to which audit criteria are met.

Control audit – the purpose of a control audit is to establish the status of correction of non-compliance and/or vulnerabilities identified during an audit.

Individual attestation of competence – document issued by an assessment centre following written and oral examinations, certifying that an auditor or audit team leader has the knowledge and skills expected under this baseline.

Auditor – individual carrying out a cyber security audit on behalf of a service provider.

Beneficiary – legal entity whose information system is the subject of the service. The beneficiary may or may not be the client of the service.

Client – legal entity contracting a service provider to provide a qualified service. The client may or may not be the beneficiary of the service.

Compliance – satisfaction of audit criteria.

Audit finding – result of the evaluation of the audit evidence gathered in relation to the audit criteria.

Service agreement – written agreement between the client and the service provider for the performance of the service.

Audit criteria – all the policies, standards, guides, procedures, requirements, recommendations, good practices, etc. used as references against which audit evidence is compared.

Audit team – group consisting of the audit team leader, the auditors and, where appropriate, experts.

Expert – individual whom the service provider may call upon to carry out part of the service when specific knowledge and skills, outside the scope of the baseline's activities and not held by the auditors, are required for the proper performance of the service. The expert may be internal or external to the service provider.

Hacktivist or isolated threat – this threat is characterised by cyber attacks carried out by a lone individual or a hacktivist group. The methods used include denial-of-service attacks and data leaks in particular. Isolated threats also include individuals using unsophisticated tools or with privileged access within an entity, but with limited resources.

Strategic threat – this threat is characterised by persistent and targeted cyber attacks carried out or financed by a state. It requires considerable technical and organisational resources, as well as discretion. These attacks may be carried out for espionage, pre-positioning or destabilisation purposes.

Systemic threat – this threat is characterised by its ability to affect a large number of entities. It includes cyber crime, involving the use of mostly opportunistic cyber attacks. These attacks are generally carried out for financial gain and may take the form of ransomware or fraud. These threats are also represented by the proliferation of offensive tools and services available off-the-shelf or marketed by private companies. These services may be used for economic intelligence or industrial espionage, or to give certain states with limited resources access to offensive capabilities.

Security measure – measure enabling a security requirement to be met, preventing or reducing the occurrence of a risk of a breach of information security or reducing its severity.

High level qualification – level of qualification that, compared with a substantial level qualification, provides a greater guarantee of the service provider's competence, the trust that can be placed in it and its ability to protect the information and media relating to the service. A high level service is recommended when the risks to the information system being serviced are high and/or when the intentional risk scenarios involve a strategic threat.

Substantial level qualification – level of qualification providing an initial level of guarantee particularly of the service provider's competence, the trust that can be placed in it and its ability to protect the information and media relating to the service. A substantial level service is recommended when the intentional risk scenarios affecting the information system being serviced involve a systemic, hacktivist or isolated threat.

Project outline – document drawn up and kept up to date by the service provider in consultation with the client, setting out the terms and conditions of the service. The project outline is generally drawn up after the service agreement has been signed.

Scope of the service – the physical, logical and organisational environment of the information system that is the subject of the service.

Attack potential – measure of the effort required to attack an information system, expressed in terms of an attacker's expertise, resources and motivation.

Service provider – legal entity providing a qualified service delivery, i.e. one that complies with the requirements of this baseline.

Audit evidence – records, statements of fact or other information that relate to the audit criteria and are verifiable.

Audit report – document drawn up by the audit team presenting the results of the service and submitted to the client at the end of the service.

Baseline – this document.

Team leader – individual within the service provider's organisation responsible for the audit service. In particular, the team leader is responsible for putting together the audit team, ensuring that the skills of the auditors and, where applicable, the experts, match the objectives, criteria, scope and activities of the service. The team leader may be an auditor.

Information systems security – safeguarding the security requirements, in particular the confidentiality, integrity and availability of information collected, stored, processed and distributed within an information system.

Subcontracting – operation whereby the service provider entrusts, under its responsibility, to a legal entity (the subcontractor) all or part of the performance of a contract concluded between the service provider and the client.

Information system – organised set of resources (hardware, software, personnel, data, procedures, etc.) used to collect, store, process and distribute information.

Audited information system – information system covered by the service.

Industrial system – a set of human and material resources whose purpose is to monitor or control technical installations (made up of a set of sensors and actuators).

Third party – individual or legal entity who is independent of the service provider, the client and the beneficiary.

Vulnerability – weakness in an information system or security measure that can be exploited by a threat.

II. Activities covered by the baseline

The activities covered by this baseline are as follows:

- architecture audit (ARCHI);
- configuration audit (CONF);
- source code audit (CODE);
- intrusion test (INTRUSION);
- organisational and physical audit (ORGAPHY).

Where a requirement is applicable to only one activity, it is preceded by a reference in square brackets identifying that activity. For example, a requirement preceded by the reference "[ARCHI]" applies exclusively to the architecture audit activity.

Where a requirement is applicable to several activities but is not applicable to all activities, it is preceded by a reference in square brackets identifying those activities. For example, a requirement preceded by the reference "[ARCHI, CONF]" applies exclusively to the architecture audit and configuration audit activities.

Where a requirement is not preceded by any reference in square brackets identifying an activity, then it is applicable to all activities.

The fully automated performance of an audit activity is not considered an activity within the meaning of the baseline.

II.1. Architecture audit

An architecture audit consists in assessing the level of compliance and/or security of an information system, in particular by analysing the choices made in positioning and implementing the hardware and software devices deployed within it. An architecture audit may be extended to the interconnections of the audited information system with third-party networks, in particular the Internet.

II.2. Configuration audit

A configuration audit consists in assessing the level of compliance and/or security of the configuration of the hardware and software devices deployed within an information system. These devices may include in particular network equipment, operating systems, applications or security products.

II.3. Source code audit

A source code audit consists in assessing the level of compliance and/or security of all or part of a software program's source code, or of its compilation and execution conditions. Any non-compliance or vulnerabilities identified may relate particularly to poor programming practices or development errors.

II.4. Intrusion test

An intrusion test consists in assessing the level of security of an information system by identifying and, if necessary, exploiting vulnerabilities. The intrusion test can be carried out in

three modes (black, grey or white box) depending on the level of information and access provided to the auditor.

The intrusion test simulates attackers who may or may not have legitimate access to the information system and can be carried out either from outside the audited information system (third-party networks, Internet, etc.) or from inside the audited system.

An intrusion test can be used to confirm vulnerabilities identified during other audit activities by exploiting them.

II.5. Organisational and physical audit

An organisational and physical audit consists in assessing the level of compliance and/or security of the governance, security policies and procedures implemented to ensure that the audited information system is maintained in secure conditions.

An organisational and physical audit may cover assessment of the protection of physical resources of the audited information system, such as physical access control systems, physical intrusion detection systems, video protection systems, natural risk prevention systems (fire, flood, etc.).

III. Qualification of service providers

III.1. Qualification procedures

The qualification of a service provider is carried out in accordance with the service qualification process (4) and attests that the service provider complies with the requirements of this baseline.

The baseline contains requirements and recommendations applicable to service providers, their staff and the service provided.

Requirements must be met by service providers to obtain qualification.

Recommendations are given as good practices and are not subject to verification to obtain qualification.

The baseline also provides recommendations for clients in Appendix 3. These recommendations are not subject to verification to obtain qualification.

An organisation may apply for qualification of an internal cyber security audit service, i.e. a service used to meet all or part of its own requirements. In this case, the qualification process and the requirements for obtaining qualification are strictly identical to those described in this baseline. The term "service provider" therefore refers to any organisation offering cyber security audit services on its own behalf or on behalf of other organisations.

A qualified service is one that complies with the approach described in section VI whose activities, described in section II, are carried out by one or more auditors complying with the requirements of section V and working for a qualified service provider complying with the requirements of section IV.

III.2. Qualification levels

There are two qualification levels for service providers: substantial and high.

Where a requirement is applicable to only one qualification level, it is preceded by a reference in square brackets identifying that level. Thus, a requirement preceded by the reference "[SUBSTANTIAL]" applies exclusively to the substantial level qualification and a requirement preceded by the words "[HIGH]" applies exclusively to the high level qualification.

Where a requirement is not preceded by a reference in square brackets identifying a qualification level, it applies to all qualification levels.

The requirements applicable to the high level qualification are, by default, recommendations for the substantial level qualification.

A service provider cannot obtain qualification for several activities at different qualification levels.

A service provider's high level qualification attests to its ability to carry out all the activities that establish its qualification at substantial level and at high level.

A service provider's substantial level qualification attests to its ability to carry out all the activities that establish its qualification at substantial level only.

Appendix 3 provides recommendations to clients on the choice of qualification level for the service.

III.3. Scope of qualification

The scope of qualification consists of one or more activities described in section II and a qualification level described in section III.2.

The service provider may apply for qualification for one or more activities and for one qualification level.

In order to be qualified according to a scope of qualification, the service provider must satisfy all the requirements of the baseline applicable to the activities and the qualification level which constitute the scope of qualification.

III.4. Qualification for national security purposes

In addition to the requirements of this baseline for high level, service providers carrying out cyber security audits for national security purposes must meet the requirements of the baseline (5).

Auditing the security of information systems for national security purposes includes, in particular, audits of critical information systems (SIIV) of operators of critical national infrastructures (OIV) as provided for in Article L1332-6-3 of the French Defence Code (6), accreditation audits of critical information systems of operators of critical national infrastructures (OIV) as provided for in annex 4 of the decrees (7) and audits of information systems handling information and media classified FR, EU and NATO, respectively, under the ministerial directions (2) (8) (9).

IV. Requirements applicable to the service provider

IV.1. General requirements

a) The service provider must be a legal entity.

b) The service provider must be subject to the law of a Member State of the European Union.

c) As a professional, the service provider has a duty to advise the client.

d) The service provider must obtain the client's consent before passing on to third parties any information or media relating to the service.

e) The service provider must provide proof that its organisation, the resources it uses to provide the service and the way it operates, particularly financially, are not likely to compromise its impartiality towards the client.

f) The service provider must provide the service impartially, in good faith and with respect for the client, its staff and its infrastructure.

g) The service provider must record and deal with complaints relating to qualified services lodged by clients, beneficiaries and, in general, all third parties.

h) The service provider must inform ANSSI without delay of any complaint lodged in relation to a qualified service and of the processing thereof.

IV.2. Personnel management

a) Before any auditor or team leader is incorporated into its teams, the service provider must check their training, knowledge, skills and professional references, as well as the veracity of their curriculum vitae.

b) Before the start of each service, the service provider must ensure that the members of the team have the knowledge and skills associated with their activities in accordance with Appendix 2.

c) [HIGH] The service provider must only use auditors and team leaders who have an individual certificate of competence to carry out the service.

   The service provider may, with the client's agreement, include in the audit team people who do not have an individual certificate of competence for the purposes of training or upgrading their skills. These people are present as observers and do not take part in performance of the service.

d) The service provider must ensure ongoing training for auditors and team leaders in order to keep their knowledge and skills in the field of information systems security up to date, and in particular those required to carry out their tasks.

e) The service provider must enable auditors and team leaders to monitor developments in order to keep their knowledge and skills up to date in the field of information systems security, and in particular those required to carry out their tasks.

f) The service provider is responsible for the methods and tools used by the audit team and for their correct use during the service.

g) The service provider must make the auditors and team leaders aware of the regulations in force within the European Union in terms of information systems security, and in particular those applicable to their tasks.

h) [HIGH] The service provider must ensure that no member of the audit team has a criminal record which is incompatible with the performance of their tasks.

IV.3. Protection of information

At the client's request, the service provider may process all or part of the information and media relating to the service on its own information system, that of the client or that of the beneficiary.

To obtain the high level qualification, the service provider must, in all cases, have an information system approved for the protection of information and media bearing the Restricted Distribution (diffusion restreinte) mark (1).

When carrying out a high level qualified service, the service provider must use its information system approved as Restricted Distribution (diffusion restreinte), whatever the marking of the information and media relating to the service.

When carrying out a substantial level qualified service, the service provider qualified at high level may choose to have, in addition to its Restricted Distribution (diffusion restreinte) information system, a second information system complying with the requirements of this section for substantial level. A service provider qualified to high level may, as part of a substantial level qualified service, at the client's request, process information and media relating to the service which do not bear the Restricted Distribution (diffusion restreinte) mark, either on its Restricted Distribution (diffusion restreinte) information system or on its second information system.

a) The service provider must draw up and keep up to date a risk assessment relating to its audit activity.

b) It is recommended that the service provider use the method (10) to assess and treat the risks relating to its audit activity.

c) The service provider must protect the integrity and confidentiality of information and media relating to the service according to their marking and level of sensitivity.

d) The service provider must apply the principle of least privilege and limit access to information and media relating to the service to only those people who have the right and need to know.

e) The service provider may need to connect the same equipment (USB key, computer, etc.) to its approved information system and to the audited information system. The service provider must implement appropriate security measures for this equipment in order to meet the operational requirements of the service and the security requirements of its approved information system. [HIGH] The service provider is not required to obtain security accreditation for the Restricted Distribution (diffusion restreinte) equipment if the information system being audited is not approved as Restricted Distribution (diffusion restreinte).

f) The service provider must obtain security accreditation for its information system.

g) [HIGH] The service provider must obtain security accreditation for its information system for the protection of information and media marked as Restricted Distribution (diffusion restreinte).

h) It is recommended that the service provider implement the approach described in the guide (11) to obtain security accreditation for its information system.

i) The service provider must be able to use its information system to carry out the entire service.

j) [HIGH] The service provider must implement all the rules of the cyber hygiene guide (12) for the enhanced level on its Restricted Distribution (diffusion restreinte) information system.

k) [HIGH] The service provider must implement all the rules relating to the protection of information systems dealing with information and media marked as Restricted Distribution (diffusion restreinte) as defined in (1) on its Restricted Distribution (diffusion restreinte) information system.

l) [HIGH] It is recommended that the service provider implement the recommendations of the guide (13) on its Restricted Distribution (diffusion restreinte) information system.

m) [SUBSTANTIAL] The service provider must implement all the rules of the cyber hygiene guide (12) for standard level on its information system.

n) The service provider must carry out a periodic review of access rights to its information system.

o) [HIGH] The service provider must carry out a review of access rights to its information system every six months.

p) The service provider must have an offline information system to store all the information and media relating to the service for which it has received authorisation to retain from the client.

V. Requirements applicable to the service provider's staff

V.1. General knowledge and skills

a) Auditors and team leaders must be familiar with good practices and the audit methodology described in the standard (3).

b) Auditors must possess the personal qualities described in section "7.2.2 Personal behaviour" of the standard (3).

c) Team leaders must possess the personal qualities described in section "7.2.3.4 General competencies of the audit team leader" of the standard (3).

d) Auditors and team leaders must have good writing and summarising skills, and be able to convey information that is relevant and appropriate to the profiles of their contacts (management, technical departments, business and security managers, etc.).

V.2. Specific knowledge and skills

a) Depending on their role, auditors and team leaders must perform the 118218AloCyber

b) in accordance with the requirements of section VI.

c) Depending on their role, auditors and team leaders must carry out the tasks described in Appendix 2.

d) Depending on their role, auditors and team leaders must have up-to-date information systems security knowledge and skills, particularly those described in Appendix 2.

V.3. Experience

a) It is recommended that auditors and team leaders have received training in information systems security.

b) It is recommended that auditors and team leaders have at least one year's experience in cyber security auditing.

V.4. Commitment

a) Auditors and team leaders must have an employment contract with the service provider.

b) The service provider must have a contractual framework with experts.

VI. Requirements applicable to the service

VI.1. Stage 1 – Preliminary qualification of suitability to carry out the service

a) On the basis of the information provided by the client, and in particular the objectives, criteria, scope, audit activities and any special terms and conditions of the service[1], the service provider must do a preliminary qualification of suitability in order to make an impartial assessment of whether it is able to carry out the service in full, in part or not at all.

b) The service provider must inform the client of the conclusions of the preliminary qualification of suitability to carry out the service and, in particular, whether it considers that it is in a position to perform the service in full, in part or not at all.

c) The service provider must only agree to provide the service if the conclusions of the preliminary qualification of suitability confirm that it is fully capable of providing the service.

VI.2. Stage 2 – Drawing up the service agreement

a) The service provider must draw up a service agreement with the client.

b) The service agreement must be signed by a legal representative of the service provider and a legal representative of the client, or any person who can bind the service provider and the client.

VI.2.1. Qualification

The service agreement must:

a) specify that the service is qualified;

b) identify the qualification level of the service;

c) identify the audit activities;

d) include the service provider's certificate of qualification;

e) [HIGH] specify that each auditor and team leader has an individual certificate of competence;

f) specify that the client may, in accordance with the service qualification process (4), submit a complaint to ANSSI when it considers that the service provider has not complied with one or more requirements of the baseline in the context of a qualified service, and emphasise that in the event of a breach by the service provider, the service provider's qualification may be withdrawn, the scope of qualification reduced, or the service provider's level of recommendation downgraded.

[1] The choice of objectives, criteria, scope, audit activities and any specific terms and conditions of the service is ultimately the responsibility of the client, but the service provider has a duty to advise on their relevance and consistency in its capacity as an information systems security professional.

VI.2.2. Terms and conditions of the service

The service agreement must:

a) provide a general description of the approach, objectives, criteria, scope and activities of the audit, as well as the terms and conditions of the service: prerequisites, milestones, deliverables, dates and locations of the service. This information may be specified and updated if necessary in the project outline or in the audit plan;

b) specify that the law applicable to the service agreement is that of a Member State of the European Union, and specify which Member State;

c) specify the rules for ownership of elements protected by intellectual property, such as the tools developed specifically by the service provider as part of the service and the deliverables of the service, in particular the audit report;

d) specify that any amendment to the service agreement must be approved by a legal representative of the service provider and a legal representative of the client, or any person who can bind the service provider and the client.

VI.2.3. Responsibilities

The service agreement must:

a) specify that the client has all ownership and access rights to the scope of the service or that it has obtained the agreement of any parties whose information systems fall within the scope of the service;

b) specify that the service provider must inform the client in writing without delay in the event of a breach of the service agreement;

c) describe the main risks relating to the service, in particular those concerning threats to the availability of the audited information system and the confidentiality of its data.

VI.2.4. Confidentiality

The service agreement must:

a) specify that the service provider will only collect and audit information and media that are strictly necessary for the proper performance of the service in accordance with the objectives, criteria, scope and activities of the service;

b) specify that the service provider will not divulge or share any information or material relating to the service to third parties without the written authorisation of the client;

c) specify that, at the end of the service, the service provider shall return, delete or destroy all information and media relating to the service, with the exception of those for which it has received authorisation to retain from the client;

d) specify that, at the end of the service, the service provider must store on an offline information system all the information and media relating to the service for which it has received authorisation to retain from the client.

VI.2.5. Experts

The service agreement must:

a) specify that the service provider may include in the audit team one or more experts to participate in the performance of certain audit activities where these require specific knowledge or skills that the auditors do not have, provided that:

   i. there is a contractual framework between the service provider and the experts;

   ii. the use of experts is accepted by the client;

   iii. the experts are duly supervised by the team leader.

VI.2.6. Subcontracting

The service agreement must:

a) specify that the service provider may subcontract all or part of the audit activities to a subcontracted service provider, provided that:

   i. the subcontracted service provider is qualified for the subcontracted audit activities;

   ii. the subcontracted service is qualified to the same level;

   iii. there is a contractual framework between the service provider and the subcontracted service provider;

   iv. the use of subcontractors is accepted by the client in the project outline.

VI.2.7. Project outline

The service agreement must:

a) stipulate the drawing up a project outline and that it must be updated during the service;

b) indicate that the project outline complies with the requirements set out in section VI.3.2.

VI.3. Stage3 – Preparing the service

VI.3.1. Setting up the team

a) The service provider must appoint a team leader.

b) [HIGH] The team leader must have a valid individual certificate of competence.

c) The team leader must put together a team of auditors and, where appropriate, experts with all the knowledge and skills required to carry out the service. The team leader may, if he has sufficient knowledge and skills, carry out the service alone.

d) The audit team leader must regularly reassess the profile and number of auditors and, if applicable, experts to ensure that the service provider's commitment remains appropriate for the proper performance of the service.

e) [HIGH] The auditors must each have a valid individual certificate of competence for the activities entrusted to them.

VI.3.2. Drawing up the project outline

a) The team leader must draw up the project outline in consultation with the audit team and the client's contact person for the service.

The project outline must:

b) specify the audit objectives, criteria, scope and activities, as well as the terms and conditions of the service: prerequisites, milestones, deliverables, dates and locations of performance, etc.;

c) identify the governance bodies for the service and specify their roles and frequency of meetings;

d) Identify the name of the client's contact person, whose role is to manage the relationship with the service provider, ensure that the service is carried out properly and that the service agreement and project outline are complied with;

e) identify whether the client authorises the service provider to subcontract all or part of the service and, if so, identify the subcontracted service provider and the subcontracted audit activities;

f) identify whether the client authorises the service provider to use experts;

g) identify the names and contact details of the members of the audit team and specify for each of them their role (team leader, auditor or expert) and the audit activities entrusted to them;

h) [HIGH] attach the individual certificates of competence of the team leader and auditors;

i) identify the names, roles and responsibilities of the persons appointed by the client and involved in the service;

j) describe any arrangements for working with third parties (subcontractors, etc.);

k) identify rights and needs for information and media relating to the service;

l) identify the marking of information and media relating to the service according to their level of sensitivity[2];

m) identify the means of protecting information and media relating to the service according to their level of sensitivity and their marking[3];

n) specify the deliverables of the service and describe the applicable terms and conditions: content, form, language, etc.;

o) identify, for each item of information and media relating to the service, which will be retained, deleted or destroyed by the service provider or returned to the client, and specify the methods of retention, deletion, destruction and return;

p) identify any specific legal and regulatory requirements to which the client is subject, in particular those applicable to the system being audited;

[2] The choice of marking of information and media relating to the service is ultimately the responsibility of the client. However, as a professional in the field of information systems security, the service provider has a duty to advise and must propose appropriate marking. Appendix 3 provides recommendations to clients on how to mark the deliverables of the service, in particular the audit report.

[3] The choice of means of protection of information and media relating to the service is ultimately the responsibility of the client. However, as a professional in the field of information systems security, the service provider has a duty to advise and must propose appropriate means of protection.

q) identify any specific requests the client may have, in particular any matters to which the client would like the service provider to pay particular attention. This may involve, for example, particular constraints to which the audited system or the client may be subject;

r) [INTRUSION] identify the intrusion test mode: black box, grey box or white box;

s) [INTRUSION] identify the attacker profiles to be simulated;

t) be validated by the client's contact person and by the team leader, and updated each time during the service.

VI.3.3. Special precautionary measures

a) The team leader must raise the client's awareness of the issues identified in Appendix 3, in particular:

   i. implementation of back-up measures for the audited information system;

   ii. [INTRUSION] managing the risks associated with intrusion tests on production or shared environments;

   iii. [INTRUSION] introduction of an intrusion test authorisation form;

   iv. implementation of security measures when the service requires the installation of tools or the execution of commands on the audited system.

b) The team leader must obtain the client's consent before carrying out any action that could lead to a malfunction or even a denial of service of the audited information system.

VI.3.4. Drawing up the audit plan

a) The team leader must draw up the audit plan in consultation with the audit team and the client's contact person.

The audit plan must describe:

b) the objectives, criteria, scope of the audit and audit activities;

c) the timetable for the service, showing the main milestones;

d) the name of the audit team leader;

e) for each of the audit activities:

   i. the names of the auditors and, where applicable, the experts responsible for carrying out the activity,

   ii. the dates and locations where the activity will take place,

   iii. any prerequisites for carrying out the activity: documents, personnel, etc.,

   iv. the audit method. The audit method must be appropriate to the audit objectives, criteria and scope, as well as to any specific requests made by the client. It must specify whether the audit activity is carried out exhaustively or by sampling, and in the latter case justify the reasons for choosing sampling and specify the sampling method: method of sample selection, sample size, etc.

VI.3.5. Opening meeting

a) It is recommended that the team leader organise an opening meeting attended by at least the team leader, the auditors, the experts if applicable, the client's contact person and the security and business managers for the information system being audited, in order to confirm their agreement to all the terms and conditions of the service, in particular the project outline and the audit plan, prior to carrying out the service.

VI.4. Stage4 – Performance of the service

VI.4.1. General requirements

a) The auditors must, in accordance with the audit objectives, criteria, scope and activities, assess the level of compliance and/or security of the information system being audited.

b) Using a risk-based approach, auditors must identify the components of the information system and the relevant documents to be audited, as well as the relevant people to be interviewed.

c) The auditors must report their audit findings to the team leader throughout the audit.

VI.4.2. Architecture audit

a) [ARCHI] The service provider must be able, in accordance with the objectives, criteria and scope of the audit, to assess the compliance and/or security of the architecture of the information system being audited by analysing, where they exist, the following documents:

   i. technical architecture documents (TADs);

   ii. OSI level 2 and 3 architecture diagrams;

   iii. flow matrices;

   iv. inventories of interconnections with third-party networks or the Internet.

b) [ARCHI] The service provider must be capable, in accordance with the objectives, criteria and scope of the audit, of evaluating the configuration of the components of the audited information system in order to assess the compliance and/or security of the architecture of the audited information system.

VI.4.3. Configuration audit

a) [CONF] The service provider must be able, in accordance with the objectives, criteria and scope of the audit, to assess the compliance and/or security of the configurations of the following elements:

   i. user directories;

   ii. physical security components (LPU, badge readers, cameras, etc.);

   iii. network components (routers, switches, etc.);

   iv. network security components (firewalls, encryption, antivirus, etc.);

   v. local security components (antivirus, *Endpoint Detection and Response* (EDR), etc.);

   vi. operating systems (servers, workstations, specific equipment);

vii. applications (business, database, web servers, etc.);

viii. cloud computing, containerisation and virtualisation environments.

VI.4.4. Source code audit

a) [CODE] The service provider must be able, in accordance with the objectives, criteria and scope of the audit, to assess the conformity and/or security of the source code of the software being audited by analysing, where they exist, the documents relating to:

i. the software specifications;

ii. the software architecture;

iii. software implementation;

iv. software administration;

v. the use of the software;

vi. software testing methods and results.

b) [CODE] The service provider must be able, in accordance with the objectives, criteria and scope of the audit, to assess the compliance and/or security of the parts of the source code of the software being audited relating to:

i. authentication mechanisms;

ii. cryptographic mechanisms;

iii. user management;

iv. access control to resources;

v. interactions with other applications;

vi. data validation.

VI.4.5. Intrusion test

The intrusion test can be carried out in one of three modes:

- black box: before starting the intrusion test, the auditors have no information about the information system being audited, with the exception of IP addresses, URLs or domain names;
- grey box: before starting the intrusion test, the auditors have some information about the information system being audited (architecture, etc.) and the permissions associated with the profiles of legitimate users of the information system who have been identified as potential attackers;
- white box: before starting the intrusion test, the auditors have as much information as possible about the information system being audited (architecture, source code, configuration, etc.) and the permissions associated with the profiles of legitimate users of the information system who have been identified as potential attackers.

a) [INTRUSION] The service provider must be able to carry out an intrusion test in three modes: black box, grey box and white box.

b) [HIGH] [INTRUSION] The service provider must be able to simulate attacker profiles with attack potentials associated with a strategic threat.

c) [INTRUSION] The service provider must be able to simulate attacker profiles with attack potentials associated with a systemic, hacktivist or isolated threat.

d) [INTRUSION] The service provider must only exploit vulnerabilities likely to render the audited information system unstable or even cause a denial of service with the written consent of the client;

e) [INTRUSION] If, at the client's request, the intrusion test is not carried out on the production environment but on another environment (test, pre-production, etc.), the service provider must check that this environment is comparable to the production environment, and check that the results of the intrusion test are applicable to the production environment.

VI.4.6. Organisational and physical audit

a) [ORGAPHY] In accordance with the objectives, criteria and scope of the audit, the service provider must assess the organisation of the information systems security.

b) [ORGAPHY] The service provider must be able to assess the organisation of the security by analysing the following documents, where they exist:

   i. risk assessment;
   ii. information systems security policy (ISSP);
   iii. security accreditation file;
   iv. disaster recovery plan (DRP);
   v. business continuity plan (BCP);
   vi. security assurance plan (SAP);
   vii. the incident management process.

c) [HIGH] [ORGAPHY] The service provider must be able to assess the physical security of the information system being audited, and in particular:

   i. physical access control;
   ii. physical intrusion detection;
   iii. video protection;
   iv. natural risk prevention: fire, flooding, etc.

VI.5. Stage 5 – Feedback

a) [HIGH] The team leader must organise an "on-the-spot" debriefing at the end of each day to present to the client's contact person:

   i. a progress report for the service;
   ii. a summary of the results of the day's audit activities;

iii. any non-compliance and/or vulnerabilities identified during the day, the exploitation of which could lead to critical risks, the associated threat scenarios and the security measures recommended to deal with these risks;

iv. any difficulties encountered during the day: difficult collaboration or unavailability of the client's or beneficiary's staff, difficulty accessing the premises, the information system or documentation, etc.

b) As soon as the audit is completed and without waiting for the audit report to be finalised, the team leader must inform the client of the findings and the initial conclusions of the audit.

c) [HIGH] As soon as the audit activities have been completed and without waiting for the audit report to be finalised, the team leader must provide the client with a written document setting out for each major non-compliance and/or vulnerability whose exploitation could lead to critical risks, the associated threat scenarios and the security measures recommended to deal with these risks.

VI.6. Stage 6 – Drawing up the report

a) The service provider must draw up an audit report[4].

VI.6.1. Qualification

The audit report must:

a) specify that the service is qualified;

b) identify the qualification level of the service;

c) identify the audit activities;

d) identify the names and contact details of the members of the audit team and specify for each of them their role (team leader, auditor or expert) and the audit activities carried out.

VI.6.2. Framework

The audit report must:

a) describe the objectives, criteria, scope of the audit and any special terms and conditions of the service;

b) identify the dates and locations of the service;

c) identify precisely (reference, version number, date, etc.) the documents on which the service provider relied to carry out the service.

VI.6.3. Executive summary

a) The audit report must include an executive summary.

The executive summary must:

[4] When several activities are carried out during the service, the choice of having one or more audit reports rests with the client.

b) be understandable by people who are not experts in information systems security;

c) provide an overall assessment of the compliance and/or security of the audited information system, correlating the results of all the audit activities;

d) describe the critical risks and associated threat scenarios exploiting the non-compliance and/or vulnerabilities identified during the audit, as well as the security measures recommended to deal with these risks;

e) describe any reservations relating to the results of the service: mismatch between objectives, criteria, scope, activities and workload, difficulties encountered during the service, sampling limitations, difficulty in collaborating with or unavailability of the client's or beneficiary's staff, difficulty in gaining access to premises, the information system or documentation, etc.;

f) recommend a control audit to verify that the security measures to deal with critical risks have been correctly implemented.

VI.6.4. Results

The audit report must:

a) uniquely identify each non-compliance and/or vulnerability identified during the audit;

b) provide the audit evidence on which the audit findings are based for each non-compliance and/or vulnerability;

c) describe each non-compliance and identify the requirement(s) not met;

d) describe each vulnerability and specify for each one: the attacker profiles, the attack scenarios, the exploitation conditions, whether an exploitation attempt was made and the result of this attempt.

e) define, in line with the audit objectives and criteria, a scale for ranking the seriousness of non-compliance and/or vulnerabilities in relation to the risks incurred;

f) propose a severity level for each non-compliance and/or vulnerability, based on the defined grading scale;

g) recommend one or more security measures for each non-compliance and/or vulnerability. These measures must be proportionate and appropriate;

h) define, in line with the audit objectives and criteria, a scale for ranking the priority of recommended security measures. This scale must at least take into account the following criteria: complexity, cost and time required to implement the security measure;

i) propose a level of priority for each security measure, based on the defined ranking scale;

j) identify, where applicable, audit activities that have been partly performed automatically;

k) identify the names and roles of the people with the client, the beneficiary and any third parties (subcontractors, etc.) with whom the service provider interacted to provide the service;

l) It is recommended that the audit report categorise each vulnerability according to a recognised nomenclature.

m) It is recommended that the service provider use the client's scale for ranking the seriousness of non-compliance and/or vulnerabilities, if the client has one.

n) It is recommended that the service provider use the client's priority ranking scale for security measures if the client has one.

VI.6.5. Appendices

The audit report must include:

a) the audit plan;

b) the project outline.

VI.7. Stage 7 – Closing the service

a) It is recommended that, once the audit report has been submitted, the team leader organise a closing meeting attended by at least the team leader, the auditors, any experts, the client's contact person, the client's management and the security and business managers of the audited information system. This meeting provides an opportunity to present a summary of the audit report and answer any questions the client may have.

b) The service provider must return, delete or destroy any information or media relating to the service for which it has not obtained the client's consent to retain in the project outline.

c) The service provider must store offline the information and media relating to the service for which it has obtained the client's consent to retain in the project outline.

d) [HIGH] It is recommended that the service provider produce a record of the destruction, deletion or return of any information or media relating to the service for which it has not obtained the client's consent to retain in the project outline. This report, which should be given to the client, should identify precisely the information or media destroyed, deleted or returned, the date and the method of destruction, deletion or return.

Appendix 1 Bibliography

1. **Instruction interministérielle n° 901 relative à la protection des systèmes d'information sensibles, n° 901/SGDSN/ANSSI, version en vigueur.** ***Disponible sur https://www.legifrance.gouv.fr.***

2. Instruction générale interministérielle n° 1300 sur la protection du secret de la défense nationale, n° 1300/SGDSN/PSE/PSD, version en vigueur. ***Disponible sur https://www.legifrance.gouv.fr.***

3. Norme internationale ISO/IEC 19011 : Lignes directrices pour l'audit des systèmes de management, version en vigueur. ***Disponible sur https://www.iso.org.***

4. Processus de qualification d'un service, version en vigueur. ***Disponible sur https://www.cyber.gouv.fr.***

5. Référentiel d'exigences applicables aux prestataires d'audit de la sécurité des systèmes d'information pour les besoins de la sécurité nationale, version en vigueur. ***Document Diffusion Restreinte, il peut être obtenu auprès de l'ANSSI.***

6. Code de la défense. ***Disponible sur https://www.legifrance.gouv.fr.***

7. Arrêtés fixant les règles de sécurité et les modalités de déclaration des systèmes d'importance vitale et des incidents de sécurité relatives aux secteurs d'activités d'importance vitale et pris en application des articles R. 1332-41-1, R. 1332-41-10. ***du code de la Défense.***

8. Instruction interministérielle n° 2102 sur la protection en France des informations classifiées de l'Union Européenne, n° 2102/SGDSN/PSD, version en vigueur. ***Disponible sur https://www.legifrance.gouv.fr.***

9. Instruction interministérielle n° 2100 pour l'application en France du système de sécurité de l'Organisation du traité de l'Atlantique nord, version en vigueur. ***Disponible sur https://legifrance.gouv.fr.***

10. Guide - Méthode de gestion de risques EBIOS Risk Manager. ***Disponible sur https://www.cyber.gouv.fr.***

11. Guide - L'homologation de sécurité en neuf étapes simples, ANSSI, version en vigueur. ***Disponible sur https://cyber.gouv.fr.***

12. ***Guide - Guide d'hygiène informatique, ANSSI, version en vigueur.*** **Disponible sur https://cyber.gouv.fr.**

13. Guide - Recommandations pour les architectures des systèmes d'information sensibles ou Diffusion Restreinte – version en vigueur. ***Disponible sur https://www.cyber.gouv.fr.***

14. Loi relative à la programmation militaire, version en vigueur. ***https://www.legifrance.gouv.fr.***

15. Directive (UE) 2016/1148 du Parlement européen et du Conseil du 6 juillet 2016 concernant les mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union. ***Disponible sur https://eur-lex.europa.eu.***

16. Directive (UE) 2022/2555 du Parlement européen et du Conseil du 14 décembre 2022 concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union. ***Disponible sur https://eur-lex.europa.eu.***

17. Référentiel général de sécurité, version en vigueur. *Disponible sur https://legifrance.gouv.fr*.

18. Règlement (UE) 2016/679 du Parlement européen et du Conseil du 27 avril 2016 relatif à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données. *Disponible sur https://eur-lex*.

19. Norme internationale ISO/IEC 27001 : Techniques de sécurité – Systèmes de gestion de la sécurité de l'information – Exigences, version en vigueur. *Disponible sur https://www.iso.org*.

20. Norme internationale ISO/IEC 27002 : Techniques de sécurité – Code de bonne pratique pour la gestion de la sécurité de l'information, version en vigueur. *Disponible sur https://www.iso.org*.

21. Guide - Guide d'achat de produits de sécurité et de services de confiance qualifiés, version en vigueur. *Disponible sur https://www.cyber.gouv.fr*.

22. Instruction interministérielle n° 910 relative aux articles contrôlés de la sécurité des systèmes d'information (ACSSI), n°910/SGDSN/ANSSI, version en vigueur. *Disponible sur https://www.legifrance.gouv.fr*.

23. Loi relative à la programmation militaire, version en vigueur. *Disponible sur https://www.legifrance.gouv.fr*.

Appendix 2 Knowledge, skills and tasks of the service provider's staff

This appendix describes the knowledge, skills and tasks of the service provider's staff.

Knowledge of the regulations cited in section I is supplemented by the specific tasks and skills required for each staff profile described in the following sections of this appendix.

To qualify, the service provider must have the following profiles for each audit activity:

Activity	Profile(s)
ARCHI	Architectural auditor
CONF	Configuration auditor
CODE	Source code auditor
INTRUSION	Intrusion testing auditor
ORGAPHY	Organisational and physical auditor

I. Knowledge of regulations

Auditors and team leaders must be familiar with the following regulations:

- protection of national defence secrets (2);
- protection of sensitive information systems (1);
- loi de programmation militaire (Critical Information Infrastructure Protection Law) (14) and in particular the provisions applicable to the critical information systems (SIIV) of operators of critical national infrastructures (OIV);
- European directives on network and information security (15) and (16);
- the General Security Baseline (17) and in particular the provisions applicable to administrative authorities;
- the General Data Protection Regulation (18);
- protection of classified information of the North Atlantic Treaty Organisation (NATO) (9);
- protection of European Union (EU) classified information (8).

II. Team leader

This section describes the tasks and skills of the team leader.

II.1. Tasks

The team leader is responsible for the following tasks:

- defining and implementing an organisation appropriate to the audit objectives, criteria, scope and activities;
- setting up an audit team comprising auditors and, where necessary, experts;
- managing and controlling the activities of the audit team;
- defining and managing service priorities;
- maintaining an up-to-date status report on the progress of the service;
- provide an overall assessment of the compliance and/or security of the audited information system, correlating the results of all the audit activities;
- providing an overall assessment of critical risks and associated threat scenarios correlating the results of all audit activities;
- providing appropriate recommendations to remedy the critical risks identified during the service;
- checking the quality and validating the deliverables of the service, in particular the project outline, the audit plan and the audit report.

II.2. Skills

The team leader must have in-depth skills in most of the areas required for the service.

III. Architectural auditor

This section describes the tasks and skills of the architecture auditor.

III.1. Tasks

The auditor must carry out the following tasks:

- adopt a global view of the audited information system, and, using a risk-based approach, identify:
  - the relevant components to be audited,
  - the relevant documents to be consulted,
  - the relevant staff to meet,
- collect and audit the relevant elements of the information system being audited;
- conduct interviews with the relevant staff;
- identify non-compliance and/or vulnerabilities in the architecture of the audited information system;
- identify the risks and threat scenarios associated with the non-compliance and/or vulnerabilities identified;
- recommend appropriate security measures to remedy identified non-compliance and/or vulnerabilities.

III.2. Skills

The auditor must have in-depth skills in the following technical areas:

- networks and protocols:
  - network protocols and infrastructures;
  - common application protocols and infrastructure services;
  - configuring and securing the main network equipment on the market;
  - telecommunications networks;
  - wireless technologies;
  - telephony.
- security equipment and software:
  - firewalls;
  - encryption;
  - backup systems;
  - shared storage systems;
  - authentication servers;
  - reverse proxy servers;
  - log management solutions;
  - intrusion detection and prevention equipment;
- special topologies:
  - cloud computing, containerisation and virtualisation;
  - mapping, inventory of flows and interconnections, associated partitioning.

When the information system being audited is an industrial system, the auditor must also have in-depth skills in the following technical areas:

- PLC-based functional architectures;
- industrial networks and protocols:
  - industrial network topologies;
  - compartmentalisation of industrial networks from other information systems;
  - transmission and communication protocols used by programmable controllers and industrial equipment (Modbus, S7, EtherNetIP, Profibus, Profinet, OPC (classic and UA), IEC 61850);
  - industrial radio and wireless technologies (including protocols based on the IEEE 802.15.4 standard);
- the functional role of the various pieces of equipment.

IV. Configuration auditor

This section describes the tasks and skills of the configuration auditor.

IV.1. Tasks

The auditor must carry out the following tasks:

- adopt a global view of the audited information system, and, using a risk-based approach, identify:
  - the information components to be audited,
  - the relevant documents to be consulted,
  - the relevant staff to meet;
- collect and audit the relevant elements of the information system being audited;
- conduct interviews with the relevant staff;
- identify non-compliance and/or vulnerabilities in the configuration of the audited information system;
- identify the risks and threat scenarios associated with the non-compliance and/or vulnerabilities identified;
- recommend appropriate security measures to remedy identified non-compliance and/or vulnerabilities.

IV.2. Skills

The auditor must have in-depth skills in the following technical areas:

- networks and protocols:
  - network protocols and infrastructures;
  - common application protocols and infrastructure services;
  - configuring and securing the main network equipment on the market;
  - telecommunications networks;
  - wireless technology;
  - telephony.
- security equipment and software:
  - firewalls;
  - encryption;
  - backup systems;
  - shared storage systems;
  - authentication servers;
  - reverse proxy servers;
  - log management solutions;

  - intrusion detection and prevention equipment;
  - client-side security software (e.g. antivirus, EDR, XDR, SOAR, etc.).
- operating systems (environment and hardening):
  - Microsoft systems;
  - UNIX/Linux systems;
  - centralised systems (based on OS400 or zOS, for example);
  - mobile systems and smartphones (based on Android or iOS);
  - virtualisation solutions.
- application layer:
  - client/server applications;
  - programming languages used for configuration (e.g. scripts, WMI filters, etc.);
  - cryptographic mechanisms;
  - application base:
    - web servers,
    - application servers,
    - database management systems,
    - software packages;
- intrusion techniques;
- special topologies:
  - cloud computing, containerisation and virtualisation;
  - partitioning and defence in depth.

When the information system being audited is an industrial system, the auditor must also have in-depth skills in the following technical areas:

- industrial networks and protocols:
  - transmission and communication protocols used by programmable controllers and industrial equipment (Modbus, S7, EtherNetIP, Profibus, Profinet, OPC (classic and UA), IEC 61850);
  - industrial radio and wireless technologies (including protocols based on the IEEE 802.15.4 standard);
- equipment:
  - configuring and securing the main PLCs and industrial equipment on the market.

V. Source code auditor

This section describes the tasks and skills of the source code auditor.

V.1. Tasks

The auditor must carry out the following tasks:

- adopt a global view of the audited information system, and, using a risk-based approach, identify:
    - the relevant components of the code to be audited,
    - the relevant documents to be consulted,
    - the relevant staff to meet;
- collect and audit the relevant elements of the information system being audited;
- conduct interviews with the relevant staff;
- identify non-compliance and/or vulnerabilities in the audited code;
- identify the risks and threat scenarios associated with the non-compliance and/or vulnerabilities identified;
- recommend appropriate security measures to remedy identified non-compliance and/or vulnerabilities.

V.2. Skills

The source code auditor must have in-depth skills in the following technical areas:

- application layer:
    - security development guidelines and principles;
    - application architectures (client/server, n-tier, etc.);
    - programming languages;
    - cryptographic mechanisms;
    - communication mechanisms (internal to the system and via the network) and associated protocols;
    - application base:
        - web servers;
        - application servers;
        - database management systems;
        - software packages;
- attacks:
    - principles and methods of application intrusion;
    - bypassing software security measures;
    - techniques for exploiting vulnerabilities and elevating privileges.
- search for the most widespread vulnerabilities, in particular:
    - *cross-site scripting (XSS);*

- SQL *(structured query language)* injection*;*
- *cross-site request forgery (CSRF);*
- application logic errors;
- memory management errors;
- execution of arbitrary commands;
- inclusion of files (local or remote).

When the information system being audited is an industrial system, the auditor must also have in-depth skills in the following technical areas:

- PLC-based functional architectures;
- SCADA application architectures (based on a software package or not);
- application architectures for user programs in industrial programmable logic controllers;
- industrial networks and protocols:
  - transmission and communication protocols used by PLCs and industrial equipment (Modbus, S7, EtherNetIP, Profibus, Profinet, OPC (classic and UA), IEC 61850).

VI. Intrusion testing auditor

This section describes the tasks and skills of the intrusion test auditor.

VI.1. Tasks

The auditor must carry out the following tasks:

- adopt a global view of the audited information system, and, using a risk-based approach, identify:
  - the relevant components to be attacked,
  - the relevant documents to be consulted,
  - the relevant staff to meet;
- identify vulnerabilities in the audited information system and, if necessary, exploit them;
- Identify the risks and threat scenarios associated with the vulnerabilities identified;
- recommend appropriate security measures to remedy identified vulnerabilities.

VI.2. Skills

The auditor must have in-depth skills in the following technical areas:

- networks and protocols:
  - network protocols and infrastructures;
  - common application protocols and infrastructure services;

  - configuring and securing the main network equipment on the market;
  - telecommunications networks;
  - wireless technologies;
  - telephony.
- security equipment and software:
  - firewalls;
  - encryption;
  - backup system;
  - shared storage system;
  - authentication server;
  - reverse proxy server;
  - log management solution;
  - intrusion detection and prevention equipment;
  - client-side security software (e.g. antivirus, EDR, XDR, SOAR, etc.).
- operating systems:
  - Microsoft systems;
  - UNIX/Linux systems;
  - centralised systems (based on OS400 or zOS, for example);
  - mobile systems and smartphones (based on Android and iOS);
  - virtualisation solutions.
- application layer:
  - security development guidelines and principles;
  - client/server applications;
  - programming languages as part of code audits;
  - cryptographic mechanisms;
  - communication mechanisms (internal to the system and via the network) and associated protocols;
  - application base:
    - web servers;
    - application servers;
    - database management systems;
    - software packages.
- attacks:
  - principles and methods of application intrusion;

- bypassing software security measures;
- techniques for exploiting vulnerabilities and elevating privileges.

When the information system being audited is an industrial system, the auditor must also have in-depth skills in the following technical areas:

- PLC-based functional architectures;
- industrial networks and protocols:
  - industrial network topologies;
  - compartmentalisation of industrial networks from other information systems;
  - transmission and communication protocols used by programmable controllers and industrial equipment (Modbus, S7, EtherNetIP, Profibus, Profinet, OPC (classic and UA), IEC 61850);
  - industrial radio and wireless technologies (including protocols based on the IEEE 802.15.4 standard);
- equipment:
  - configuring and securing the main PLCs and industrial equipment on the market.

VII. Organisational and physical security auditor

This section describes the tasks and skills of the organisational and physical security auditor.

VII.1. Tasks

The auditor must carry out the following tasks:

- adopt a global view of the audited information system, and, using a risk-based approach, identify:
  - the relevant components of the information system to be audited,
  - the relevant documents to be consulted,
  - the relevant staff to meet,
  - the relevant premises to be audited;
- collect and audit the relevant elements of the information system being audited;
- conduct interviews with the relevant staff;
- audit the security of the premises;
- identify non-compliance and/or vulnerabilities;
- identify the risks and threat scenarios associated with the non-compliance and/or vulnerabilities identified;
- recommend appropriate security measures to remedy identified non-compliance and/or vulnerabilities.

VII.2. Skills

The auditor must have in-depth skills in the following areas:

- mastery of technical baselines:
- mastery of the regulatory framework:
    - standards (19) and (20);
    - regulatory texts relating to information systems security, audits and related subjects[16].
- expertise in areas relating to the organisation of information systems security:
    - risk assessment;
    - information systems security policy (ISSP);
    - chains of responsibility in information systems security;
    - human resources security;
    - managing the operation and administration of the information system;
    - logical access control to the information system;
    - application development and maintenance;
    - information security incident management;
    - business continuity plan management;
    - physical security.
- mastery of audit-related practices:
    - conducting interviews;
    - site visit;
    - documentary analysis.

When the information system being audited is an industrial system, the auditor must also have in-depth skills in the following technical areas:

- functional security standards such as IEC 61508
- specific standards on industrial automation and control systems, such as IEC 62443;
- PLC-based functional architectures;
- roles and use of industrial protocols;
- knowledge of the functional role of different equipment.

[16] In particular, rules relating to the protection of privacy, professional secrecy, private correspondence or personal data, attacks on the fundamental interests of the nation, terrorism, attacks on public confidence, intellectual property, the use of cryptology and the national scientific and technical heritage.

Appendix 3 Recommendations for clients

This appendix lists ANSSI's recommendations for clients of cyber security audit services.

I. Before the service

a) When the client is an administrative authority or an operator of vital importance, it may ask ANSSI to take part in defining the specifications of a call for tenders or a contract for a cyber security audit.

b) It is recommended that the client use the guide (21) to draw up the specifications for a call to tender or a contract for a cyber security audit.

c) The client can consult the catalogue of qualified service providers on the ANSSI website. For each service provider, this catalogue sets out the activities for which it is qualified, the period of validity of the qualification, the level of qualification and the level of recommendation.

d) Qualified service providers retain the option of carrying out non-qualified services, but may not claim qualification for these services. If the client wishes to benefit from a qualified service, i.e. one that complies with the requirements of this baseline, it must ensure that the service agreement drawn up with the service provider explicitly states that the service is qualified.

e) An unqualified service, i.e. one that does not comply with the requirements of this baseline, exposes the client to certain risks, in particular compromising confidential information and the loss or unavailability of the information system that is the subject of the service. These risks can be reduced by using a qualified service provider. If, however, the client does not wish to use a qualified service, it is nevertheless recommended that they ask the service provider for a document identifying all the requirements of this baseline that have not been met as part of their service, in order to identify the risks to which they are exposed.

f) If the client wishes to use a cyber security audit service provider (PASSI) and a cyber security support and consultancy service provider (PACS) for the same scope, it is recommended that PASSI and PACS be two separate service providers in order to guarantee a higher level of impartiality and independence.

g) The client may, in accordance with the qualification process for a service (4), submit a complaint to ANSSI when it considers that the service provider has not complied with one or more requirements of this baseline in the context of a qualified service. Complaints may also be lodged directly with the qualified service provider, which is obliged to inform ANSSI without delay.

   If, after investigating the complaint, it is found that the qualified service provider has failed to comply with one or more requirements of this baseline in the context of a qualified service, the service provider's qualification may be withdrawn, the scope of qualification reduced, or the level of recommendation of the service provider downgraded in accordance with the qualification process for a service (4).

h) Unless the client is subject to a legal, regulatory or contractual obligation, the choice of qualification level for the service is the sole responsibility of the client. In this case, it is

recommended that the qualification level of the qualified service be determined using a risk-based approach.

It is recommended that a high level service be carried out when the risks to the information system being serviced are high and/or when the intentional risk scenarios involve strategic threats. In other cases, a substantial level service should suffice.

For this reason, in the case of a high level qualified service, it is recommended that the client require of the service provider in the project outline that the audit report bear the words Restricted Distribution (diffusion restreinte).

i) Where the information system to be provided is a national security system, the client must provide a service that is qualified for national security purposes, i.e. in addition to the requirements for high level of this baseline, it must comply with the requirements of the baseline (5).

j) The qualification of a service provider does not attest to its ability to access or hold classified information and therefore does not replace the clearance of a legal or natural person under the directive (2).

Where the service requires the service provider to access or hold classified information, the client must check that the service provider and its staff comply with the principles governing access to national defence secrets by natural and legal persons.

k) The qualification of a service provider does not attest to its ability to access or hold controlled items of information systems security (ACSSI) (22).

Where the service requires the service provider to access or hold controlled items relating to information systems security, the client must check that the service provider has the necessary DACSSI (Decisions on Access to ACSSI) for classified ACSSI or training certificates for the handling of ACSSI for unclassified ACSSI.

l) It is recommended that the client determine the objectives, criteria, scope and activities of the service using a risk-based approach.

m) It is recommended that the client ask the service provider to provide references of services carried out with objectives, criteria, scope and activities similar to those required by the client.

n) Audits should be as exhaustive as possible, while taking account of the client's time and budget constraints.

The service provider must propose a workload appropriate to the objectives, criteria, scope and activities, although the workload ultimately chosen is the sole responsibility of the client. The service provider will mention in the audit report any reservations about the service that may have an impact on the results of the audit, particularly in the event of a mismatch between the workload and the objectives, criteria, scope and activities.

o) In order to reduce the workload of the service and therefore its cost, while still meeting the objectives of the service, the service provider can propose that the client carry out sampling using a risk-based approach.

p) The client must appoint a contact person whose role is to draw up and keep up to date, in collaboration with the service provider, the project outline for the service. The contact

person manages the relationship with the service provider and ensures that the service is carried out correctly, in compliance with the service agreement and the project outline.

It is recommended that the client's contact person have the means to engage the responsibility of the client and to respond rapidly to the service provider's requests.

q) [INTRUSION] It is recommended that the intrusion test activity never be carried out on its own, but should always be complemented by configuration auditing, architecture auditing and, if necessary, source code auditing.

r) [INTRUSION] Whenever possible, it is recommended that intrusion tests be carried out on a test or pre-production environment rather than on a production environment in order to avoid the consequences of any disruption to the system being audited.

s) [INTRUSION] It is recommended that intrusion tests not be carried out on shared environments unless agreed by the hosting provider and after the risks have been assessed and controlled, and responsibilities have been clearly established.

t) [ARCHI, CONF, CODE] It is recommended that architecture, configuration, source code, organisational and physical audits be carried out on production environments.

u) [INTRUSION] It is recommended that, before carrying out an intrusion test, the client require the service provider to draw up an authorisation form signed by the auditee, identifying in particular: the list of targets audited (IP addresses, domain names, URLs, etc.), the list of IP addresses from which the intrusion tests originate, the dates and times of the intrusion tests, and the duration of the authorisation.

II. During the service

a) It is recommended that the client authorise the service provider in the project outline to keep the audit report at the end of the service when a control audit is planned to check that the non-compliance and/or vulnerabilities recorded in the audit report have been corrected.

b) In the case of a substantial level qualified service carried out by a service provider qualified to high level, it is recommended that the client, in the project outline, require the service provider to process all information and media relating to the service on its Restricted Distribution (diffusion restreinte) information system, regardless of the marking of this information and media.

c) It is recommended that the client take measures to safeguard the audited information system before and during the audit. This must be done in collaboration with the service provider so as not to disrupt the service.

d) It is recommended that, throughout the service, the client inform the service provider of any actions it carries out on the audited information system (administration operations, back-up, restoration, etc.) that could affect the service.

e) It is recommended that, where the service requires the installation of a tool or the execution of a command on the system being audited, the client carry out these actions itself or, failing that, authorise the service provider to carry out these actions with dedicated accounts benefiting from the principle of least privilege and under the constant supervision of the client.

III. After the service

a) It is recommended that the client call on a qualified consultancy and support service provided by a qualified cyber security consultancy and support service provider (PACS) to implement the security measures proposed by the cyber security audit service provider (PASSI) and to help with their implementation.

b) It is recommended that the client carry out a control audit to check that the security measures used to correct the non-compliance and/or vulnerabilities identified during the audit have been correctly applied and effectively achieve the targeted level of compliance and/or security.

   It is recommended that the control audit be carried out as part of a qualified audit by a qualified audit service provider and that the service provider carrying out the control audit be the same service provider who carried out the initial audit.