Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

Prime Minister

The French Networks and Information Security Agency

Agence nationale de la sécurité des systèmes d'information

Security incident detection service providers
Prestataires de détection des incidents de sécurité

Requirements reference document
Référentiel d'exigences

Version 1.0 dated 6 october 2015

VERSION HISTORY

DATE	VERSION	DOCUMENT HISTORY	AUTHOR
20/03/2014	0.1	*Draft version presented in Working Group Meeting 1*	ANSSI
16/04/2014	0.2	*Draft version presented in Working Group Meeting 2*	ANSSI
03/06/2014	0.3	*Working version prepared for Working Group Meeting 3*	ANSSI
25/06/2014	0.4	*Working version prepared for Working Group Meeting 4*	ANSSI
22/07/2014	0.5	*Working version prepared for Working Group Meeting 5*	ANSSI
05/09/2014	0.6	*Working version prepared for Working Group Meeting 6*	ANSSI
10/10/2014	0.7.4	*Working version prepared for internal revisions by ANSSI*	ANSSI
25/11/2014	0.8	*Working version prepared for internal revisions by ANSSI*	ANSSI
17/12/2014	0.9.1	*Version published for public call for comments*	ANSSI
06/10/2015	1.0	*Revised version following the call for comments*	ANSSI

Comments on this document should be sent to:

The French Networks and
Information Security Agency
SGDSN/ANSSI
51 boulevard de La Tour-Maubourg
75700 Paris 07 SP
qualification@ssi.gouv.fr

CONTENTS

I. Introduction

I.1. General overview

I.1.1. Context

The growing interconnection of networks and the requirements of dematerialisation leave information systems vulnerable to cyber-attacks. The points of interconnection with external networks and, in particular, with the Internet, are all access points an attacker can attempt to exploit to enter and remain inside an information system in order to steal, alter or destroy its information assets.

The use of security incident detection systems contributes to the protection of information systems from the threats of cyber attacks. Human, technical and organisational resources can be concentrated within a cyber-security operations centre[1] dedicated to the detection of security incidents. Depending on the challenges, needs and resources of the commissioning entity, this centre can be internal, outsourced, dedicated or even shared. In this latter case, the pooling of resources can have positive effects, such as the sharing of information on threats and detection rules.

When the provision of this service is compliant with the "state of the art", and is precisely adapted to the needs of the commissioning entity, it helps to prevent severe security incidents or, when such incidents occur, to limit their consequences by making it possible to take rapid remediation actions that can be carried out by a qualified security incident response service provider (*Prestataire de Réponse aux Incidents de Sécurité* - PRIS).

However, the concentration and pooling of detection capabilities make the cyber-security operations centre a prime target for attackers. Therefore, special attention should be paid to protecting its infrastructure.

ANSSI is currently conducting an experimental procedure with selected service providers to test in real conditions the applicability of this document. At the end of this procedure, it may be modified which will lead in the publication of a new version.

I.1.2. Purpose of the document

This document is the requirements reference document applicable to a security incident detection service provider (*Prestataire de Détection des Incidents de Sécurité* - PDIS), hereinafter referred to as "the service provider".

Its purpose is to enable the approval of this category of service providers in accordance with the terms set out in section III.

It covers the different types of cyber-security operations centres[1] dedicated to the detection of security incidents: internal, outsourced, dedicated or shared.

It gives to the commissioning entity assurance regarding the competencies of the service provider and its staff, the quality of its services, and the confidence that the commissioning entity can place in the service provider, in particular with regard to confidentiality.

It can also be used, in the interest of adopting best practices, independently of any regulatory framework.

It does not exclude either the application of national laws and regulations, or the application of general rules imposed on service providers as professionals and in particular to their duty to advise their commissioning entities.

[1] Hereinafter referred to as the "security incident detection service".

I.1.3. Document structure

Section I is the introduction to this reference document.

Section II describes the activities to which this reference document relates.

Section III presents the approval methods, which attest to the compliance of the security incident detection service providers against applicable requirements.

Section IV presents the requirements applicable to service providers.

Annex 1 presents references in terms of laws, regulations, standards and other documents cited in this reference document.

Annex 2 presents the tasks and skills expected from the service provider's employees.

Annex 3 presents the recommendations for the commissioning entities when contracting with security incident detection service providers.

I.2. Document identification

This reference document is named "Security incident detection service providers – requirements reference document" *(Prestataires de détection des incidents de sécurité – référentiel d'exigences)*. It can be identified by its name, version number and date of update.

I.3. Definitions and acronyms

I.3.1. Acronyms

The acronyms used in this reference document are:

ANSSI	The French Networks and Information Security Agency *(Agence nationale de la sécurité des systèmes d'information)*
CERT-FR	The French national Computer Emergency Response Team *(Centre gouvernemental de veille, d'alerte et de réponse aux attaques informatiques*)[2]
PASSI	Audit service provider for information system security *(Prestataire d'audit de la sécurité des systèmes d'information)*
PDIS	Security incident detection service provider *(Prestataire de détection des incidents de sécurité)*
PRIS	Security incident response service provider *(Prestataire de Réponse aux Incidents de Sécurité)*
PSCE	Electronic certificate service provider *(Prestataire de service de certification électronique)*

I.3.2. Definitions

The definitions below are primarily taken from the following standards: [ISO27000] and especially [ISO27035] on the management of security incidents as well as the French national digital security strategy [STRAT_NUM].

Administrator – a member of the detection team in charge of the technical administration of the detection service devices (for example, the management of infrastructures, systems, databases, the installation of new applications, etc.).

[2] http://www.cert.ssi.gouv.fr

Collection source – equipment within the information system that generates events related to the security of the information.

Collector – a device enabling the centralisation of security events originating from various sources. In the context of this service, local collectors are the collectors installed in the commissioning entity's information system, and central collectors are the collectors used for centralising events and located in the service provider's information system.

Commissioning entity – an entity that uses a security incident detection service.

Detection rule – a list of technical elements which allows the identification of an incident based on one or more events. A detection rule may be formed by one or more markers, one or more signatures or a behavioural rule based on abnormal behaviour. A detection rule may originate either from the vendor of the technical analysis tools used for the detection service, or the service provider itself (monitoring of new incidents, a rule used for another commissioning entity, etc.), or it may have been created specifically for the commissioning entity.

Effectiveness – the level of achievement of planned activities and the expected results.

Event related to information security – an identified occurrence of a system, service or network state indicating a possible breach of information security, policy or a failure of controls, or a previously unknown situation that may be security relevant.

Information system – an organised set of resources (hardware, software, personnel, data and procedures) for processing and communicating information.

Investigation – a process designed to collect and analyse all of the technical, functional or organisational elements of the information system in order to understand the operating process and the scope of a security incident in an information system.

Operator – a member of the detection team in charge of operating the detection service (managing the detection rules, the support service, etc.). In this capacity, operators are responsible for identifying, analysing and qualifying security incidents.

Probe – a technical device designed to generate network events and/or to identify abnormal, suspicious or malicious activity on the analysed target (e.g. network traffic). A probe is considered to be a collection source within the security incident detection service.

Qualifying a security incident – determining the nature and severity of a security incident.

Reporting – the act of informing the commissioning entity of the occurrence of a security incident jeopardising its information system.

Security incident – a single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security.

Security of an information system – all of the technical and non-technical controls that make it possible for an information system to manage events that could compromise the availability, integrity or confidentiality of the data that is handled or transmitted and the related services that these systems provide or make available.

Service agreement – a written agreement between a commissioning entity and a service provider for the delivery of the security incident detection service. When the service provider is a private entity, the service agreement includes the contract form.

Service provider – an entity that provides a security incident detection service in compliance with this reference document.

Severity of a security incident – the level of impact of the security incident affecting the commissioning entity's information system.

State of the art – the set of publicly accessible best practices, technologies and reference documents (and the information that is clearly derived from them) relating to information systems security. These documents may be made available on the Internet by the information systems security community, distributed by reference or regulatory entities.

Subcontracting – an operation through which the service provider entrusts to another entity all or part of the execution of a contract concluded with the commissioning entity.

Third party – a person or organisation that is recognised as independent from the service provider and the commissioning entity.

Vulnerability – weakness of an asset or control that can be exploited by one or more threats.

II. General description of the detection service

II.1. Activities of the security incident detection service

The security incident detection service is composed of three distinct activities:

- incident management, meaning all of the technical and organisational means for identifying and qualifying a security incident on the basis of collected events. The storage of security incidents, and capitalising on them in order to improve the service is also part of this activity;
- event management, meaning all of the technical and organisational means for ensuring the collection and storage of security events;
- reporting management, meaning all of the technical and organisational means that make it possible to inform the commissioning entity about detected security incidents and to store these reports.

Reaction and remediation activities are beyond the scope of this service. Those are handled by the security incident response service providers (PRIS).

II.2. Architecture of the security incident detection service

This document does not impose any specific architecture for the detection service. The service can be implemented in a number of different ways. In particular, the commissioning entity's information system can host a significant part of the information system of the security incident detection service, provided that the requirements of the reference document are met.

The diagram below is a simplified representation of a typical architecture for a security incident detection service. This diagram is provided for illustrative purposes only and does not preclude the implementation of other service architectures.

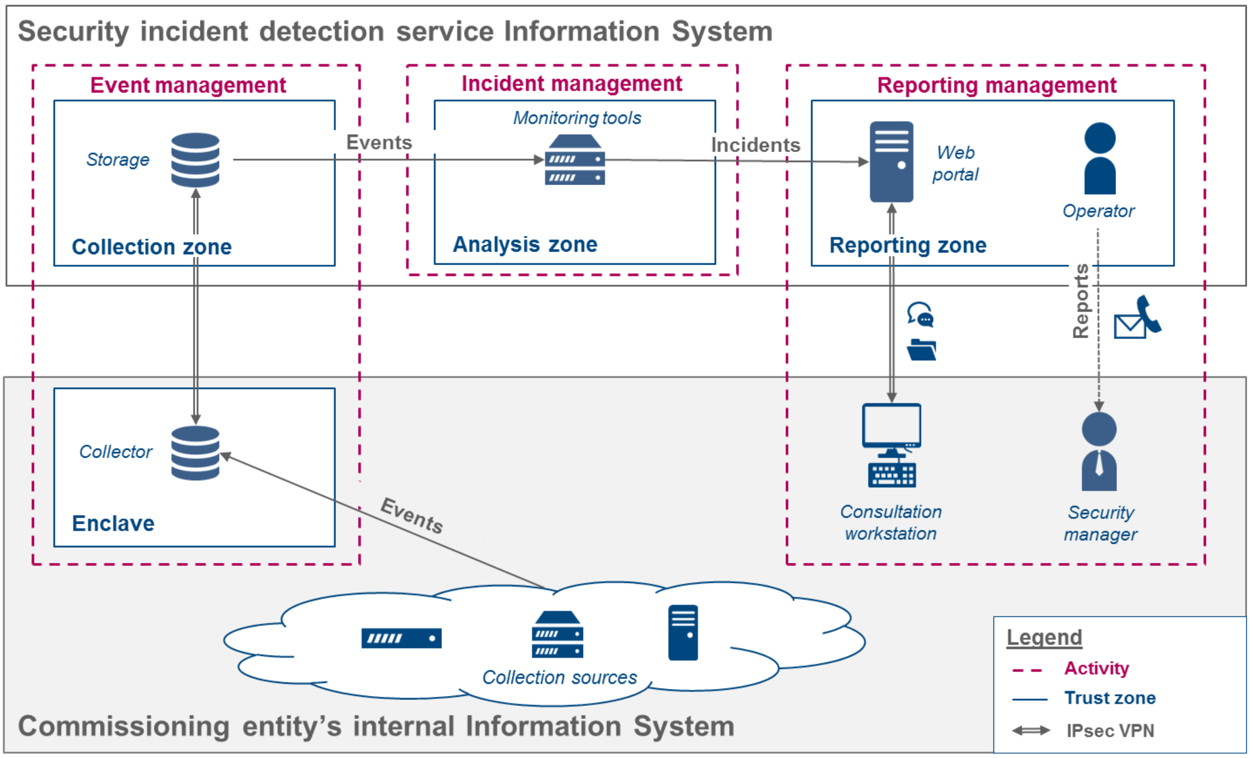

Figure 1: Illustrative diagram of the architecture of a security incident detection service

The information system of a security incident detection service is organised into trust zones, partitioned using filtering, authentication and access control mechanisms. The trust zones are the following:

- a collection zone, comprising all the devices involved in the collection process, including the collectors and the systems for storing events;
- an analysis zone, comprising all of the devices involved in the analysis process, including the technical tools for analysing and managing the service provider's internal security incident tickets;
- a reporting zone, comprising all of the devices involved in the collection process, including the Web portal and the reporting system;
- one or more administration zones, comprising all of the administration tools and administration workstations;
- an operations zone, comprising the operators' workstations;
- an Internet zone, comprising the workstations that are authorised to access the Internet;
- one or more specific trust zones in the commissioning entity's internal information system, hereinafter referred to as enclaves. At the very least, an enclave must be established for hosting the collection devices for the detection service deployed by the commissioning entity. In particular, the enclave will contain one or more collectors, the role of which is to centralise the security events from the collection sources that are deployed on the commissioning entity's information system.

II.3. Scope of application of the requirements of the reference document

Section IV.1 lists the general requirements relating to the service provider's legal obligations, including its duties vis-à-vis the commissioning entity, its guarantees, etc.

Section IV.2 lists the requirements relating to the content of the activities of the security incident detection service:

- the requirements relating to the incident management activity, including the skills of the operators, the features of the tools used, the implementation of the detection rules, etc.
- the requirements relating to the event management activity, including the sources of collection, the centralisation of events on a collector, etc.
- the requirements relating to the reporting management activity, including the means of reporting, the consultation of incident tickets, etc.

Section IV.3 lists the requirements relating to the protection of information, including the filtering between the trust zones, the separation of roles between administrators and operators, etc.

Section IV.4 lists the requirements relating to the organisation of the service provider and the governance of the service, including the establishment of a code of ethics and recruitment, the content of the operational and strategic committee meetings, etc.

Section IV.5 lists the requirements relating to the quality and level of service, including the nature of the indicators to be monitored, the content of the service agreement established between the service provider and the commissioning entity, etc.

III. Approval of security incident detection service providers

III.1. Approval methods

The reference document contains the requirements and recommendations for security incident detection service providers.

The approval of a service provider is performed in accordance with the approval process for a trust service provider [PROCESS_QUALIF] and makes it possible to demonstrate that the service provider is compliant with the requirements of the reference document.

An organization can ask for the approval of its internal security incident detection service, that is to say a service used to fulfil, either fully or partially, its own security incident detection needs. In such a case, the approval process and the applicable requirements to obtain the approval are strictly identical to the ones defined in this reference document. The expression “service provider” can therefore refer to either an organization offering a security incident detection service internally or to other organizations.

Service providers must comply with the requirements in order to obtain the approval.

The recommendations to obtain the approval are provided as a matter of best practice and are not subject to verification.

The reference document also provides recommendations for commissioning entities in Annex 3. These recommendations are not subject to verification in the approval process.

III.2. Scope of the approval

In order to be qualified, service providers must meet all the requirements of this reference document.

In order to be qualified under the military programming law *(Loi de programmation militaire)*, service providers must comply with the requirements set out in [PDIS_LPM], in addition to the requirements defined in this reference document.

Services that meet all the requirements of this reference document are considered to be qualified services according to the meaning of the reference document.

Services that meet all the requirements of this reference document and the additional requirements of the military programming law as defined in [PDIS_LPM] are considered to be qualified services according to the meaning of the military programming law.

Qualified service providers retain the ability to provide services outside the scope for which they are qualified, but cannot, in this case, use this approval status for the purpose of providing these services.

A qualified security incident detection service can be combined with other complementary services (development, integration of security products, etc.) without losing the benefit of the approval. A qualified security incident detection service provider can, for example, be qualified for other trust service provider categories (PASSI, PRIS).

III.3. Warning

The use of non-qualified incident detection services may potentially leave the commissioning entity vulnerable to certain risks, such as the leakage of confidential information, being compromised by another of the service provider’s commissioning entities, and loss or unavailability of service. Accordingly, in the case of a non-qualified service, it is recommended that the commissioning entity request from its service provider a document listing all the requirements of this reference document that are not covered as part of its service, in order for the commissioning entity to understand the risks to which it is exposed.

IV. Requirements to be met by the service provider

IV.1. General requirements

a) The service provider must be an entity or part of an entity that has a legal personality so that it can be held legally responsible for the services that it provides.

b) The service provider must comply with the laws and regulations in force within the national territory of France.

c) The service provider must describe the organisation of the security incident detection activity that it provides to the commissioning entity.

d) The service provider has, in its professional capacity, a duty to advise vis-à-vis the commissioning entity.

e) The service provider must take responsibility for the activities it performs on behalf of the commissioning entity in connection with the service that it provides, and in particular for any damages caused to the commissioning entity. In this respect, the service provider must specify the types of damages involved and the terms under which the responsibilities are shared in the service agreement, taking into account any and all outsourced activities.

f) It is recommended that the service provider retain responsibility for the actions that it performs itself in providing the service.

g) The service provider must obtain professional liability insurance covering any damages caused to the commissioning entity and especially to its information system during the provision of the service.

h) The service provider must ensure that the consent of the commissioning entity has been obtained prior to any disclosure of information obtained or produced during the provision of the service.

i) The service provider must ensure that the information it provides, including advertising, is neither false nor misleading.

j) The service provider must provide sufficient evidence that the way in which it operates, especially in terms of its financial operations, is not liable to compromise its impartiality or the quality of its performance with respect to the commissioning entity or to cause conflicts of interest.

k) The service provider must provide the service impartially, in good faith and with respect of the commissioning entity, its employees and its infrastructure.

l) The service provider must possess valid licences for the tools (software and hardware) used to provide the service.

m) The service provider must ask the commissioning entity to notify it of any specific legal or regulatory requirements to which it is subject, especially those related to its sector of activity.

n) The service provider must inform the commissioning entity when the commissioning entity is required to report a security incident to a government authority and must assist it in this process if the commissioning entity asks it to do so.

o) The service provider must establish a service agreement with the commissioning entity. The service agreement must comply with the requirements of section IV.5.3 and must be formally approved in writing by the commissioning entity before the service is performed.

IV.2. Activities of the security incident detection service

IV.2.1. Incident management

a) The service provider must establish with the commissioning entity a list of feared incidents and the impacts and consequences associated with them based on the results of a risk assessment prepared by the commissioning entity. The service provider must recommend to the commissioning entity that it updates its risk assessment in the event of a change in its infrastructure.

b) The service provider must be able to take into account *at a minimum* the following categories of feared security incidents:

- exploitation of a vulnerability;
- elevation of privileges;
- data exfiltration;
- viral propagation;
- use of a persistence mechanism;
- denial of service;
- unauthorised access to a resource;
- identity theft;
- actions that do not comply with the commissioning entity's security policy.

c) It is recommended that the service provider take into account the list of security incidents and their origins in Annex B of [ISO27035] and [ETSI_ISG_ISI].

d) The service provider must develop and implement with the commissioning entity an analysis strategy that makes it possible to detect all the incidents on the feared incident list (see requirement IV.2.1.a). The analysis strategy must be reviewed with the commissioning entity during the operational committee meetings defined in section IV.4.3.

e) The analysis strategy must include a precise description of the implementation of the detection rules for detecting security incidents based on the collected events.

f) The service provider must create detection rules based on:

- the list of security incidents that are feared by the commissioning entity;
- the knowledge bases acquired from vendors and specialist information systems security companies;
- the internal knowledge bases derived from the expertise of the service provider:
    - the monitoring and qualifying of vulnerabilities, with priority given to those relating to the execution of arbitrary code, locally or remotely;
    - the monitoring and qualification of command control protocols;
    - the monitoring of the modes of operation for attacks and malicious code.
- the contextual elements specific to the commissioning entity;
- the rules provided directly by the commissioning entity, previously validated by the service provider;
- the security incidents detected with any other commissioning entities.

g) The service provider must develop and implement a marking policy for detection rules. This policy must define, for each detection rule:

- a unique identifier for the detection rule;
- the owner of the detection rule, meaning the entity that owns the rights on the detection rule;
- the author of the detection rule, meaning the entity that created the detection rule;
- the source of the detection rule, meaning the entity that is the source of the information enabling the creation of the detection rule and which is not necessarily the owner or author of the detection rule;
- the creation date of the detection rule;
- the description of the detection rule;
- the phases of attack detected by the rule, such as: reconnaissance, initial infiltration, interaction with command and control infrastructure, elevation of privileges, lateral movements, exfiltration, etc.;
- the level of sensitivity or classification of the detection rule;
- the terms for the distribution of the detection rule, such as "unrestricted distribution", "may be distributed within a community but not publicly", "may be distributed internally subject to need-to-know", "may be distributed to named individuals and may not be redistributed";
- the terms for managing the signature rule;
- a description of the method of analysis for events;
- whether or not it is possible to conduct open-source research;
- the descriptions and/or identifiers (e.g. CVE) of vulnerabilities for which exploitations or exploitation attempts have been detected by the rule;
- the instructions to be followed in the event that the detection rule is triggered.

h) The service provider must establish and keep up to date, for each commissioning entity, a list of all detection rules that have been implemented or that are being implemented as part of the service. This list must identify, for each detection rule:

- the date on which the detection rule was included in the technical analysis tools;
- if the service provider has conducted an *a posteriori* analysis with this detection rule (see requirement IV.2.1.y) and the date of this analysis, if applicable;
- the date on which the detection rule was withdrawn from the technical analysis tools in use.

This list must make it possible to establish a historical record for the detection rules. A detection rule that has been withdrawn from the technical analysis tools in use must therefore be marked as withdrawn and must not be deleted from this list.

i) The service provider must send to the commissioning entity, *at a minimum* once a month, a detection rule status report that presents:

- the number of detection rules created, modified or withdrawn from the analysis tools in use;
- the identifier and description of each rule that has been created, modified or withdrawn from the analysis tools in use;
- the reason for the creation, modification or withdrawal of the security rule (e.g. creation, modification or withdrawal at the request of the commissioning entity, etc.).

It is recommended that the service provider send the detection rule status report to the commissioning entity once a week.

j) The service provider must implement in the technical analysis tools in use all of the detection rules identified in the list set out in requirement IV.2.1.h) except for the rules marked as withdrawn.

k) The service provider must independently add the new detection rules to the technical analysis tools in use.

   Following an addition of this type, the service provider must update the documentary record and provide information about the details of the additions that have been made.

l) The service provider must, in the event that it is difficult or impossible to implement a detection rule, notify the commissioning entity as soon as possible and no later than fifteen days after the decision to implement the detection rule, and specify the reasons for the failure to implement the rule.

m) The service provider must qualify the detected security incidents in order to assess their veracity (false positive or real incident) and severity (functional impacts, informational impacts, etc.).

n) The service provider must establish with the commissioning entity a severity scale associated with the feared security incidents, taking into account the risk assessment and especially the threats, the assets, the potential impacts and their level of severity.

o) It is recommended that the service provider use the severity scale for information security incidents in Annex C of [ISO27035].

p) The service provider must be able to integrate the results of the tests for vulnerabilities and intrusions carried out by the commissioning entity on its information system.

q) The service provider must create a ticket for each security incident detected and make it available to the commissioning entity. *At a minimum*, the security incident ticket must contain the following elements:

   - the date and time when the security incident was detected;
   - the description of the security incident;
   - the severity of the security incident;
   - the impact of the security incident for the commissioning entity;
   - the identifiers of the detection rules that were triggered;
   - the equipment that collected the events of the incidents;
   - the identifiers of events that made it possible to detect the incident;
   - the risk resulting from the incident.

r) The service provider must define the format of the security incident tickets together with the commissioning entity.

s) It is recommended that the service provider use the security incident ticket format set out in [ETSI_ISG_ISI].

t) The service provider must have a tool for managing the security incident tickets within the analysis zone.

u) The service provider must store all of the security incidents that are confirmed or that are in the process of being qualified in one central location.

v) The service provider must be able to retrieve the events at the origin of a detected security incident throughout the retention period of the collected events.

w) The service provider must implement and keep up to date a centralised, chronological record for each commissioning entity identifying all detected security incidents.

x) The service provider must implement a process for managing the storage capacity for the security incidents that enables the service provider to monitor its evolution and to modify it in accordance with the needs of the commissioning entity.

y) The analysis strategy must ensure that for each detection rule that is created or modified, the service provider conducts an *a posteriori* analysis, meaning an analysis of all of the events that have been stored for a period of time determined together with the commissioning entity in the analysis strategy.

This requirement does not apply to detection rules requiring types of events that are not yet present in the event storage systems.

z) The service provider must be able, upon request of the commissioning entity, to conduct an analysis on the set of events that have been stored for the previous six months.

IV.2.2. Event management

a) The service provider must develop, together with the commissioning entity, and implement a collection strategy based on the list of feared security incidents (see requirement IV.2.1.a). The collection strategy must be reviewed with the commissioning entity at the operational committee meetings defined in section IV.4.3.

b) The collection strategy must identify the list of collection sources, collectors, events to be collected, describe the collection methods, and identify the frequency of collection.

c) The service provider must be, *at a minimum*, capable of collecting events from the following collection sources:

- security equipment: network firewalls, application firewalls, encrypters, probes approved by ANSSI at the appropriate level, antivirus software, authentication servers, VPN concentrators, SSL gateways, proxies, reverse proxies;
- network equipment: routers, switches, netflow, DNS servers, load balancers, time servers;
- infrastructure servers: authentication, directories, software distribution, remote management, supervision, virtualisation, file servers, backups, mail, print;
- business servers: web servers, databases, file servers, collectors;
- workstations: main operating systems;
- mobile devices.

d) The service provider must be able, *at a minimum*, to create a log for each collection source identified in requirement IV.2.2.c) of the events identified in Annex A of the ANSSI technical note on the implementation of a logging system [NT_JOURNAL].

e) The service provider must exercise its duty to advise the commissioning entity in respect of the development, implementation and review of the collection strategy. In this capacity, it must advise the commissioning entity on the development and review of the logging policy (types of events to be logged, retention periods, standardisation of information, synchronisation of time sources, etc.) and on the deployment of logging devices on the commissioning entity's information system.

f) The service provider must recommend to the commissioning entity that it integrates the deployment of probes at each of the interconnections of the commissioning entity's information system into the collection strategy, and in particular, the interconnections with:

- the Internet;
- third-party information systems (partners, subcontractors, etc.);
- the commissioning entity's other information systems with a lower or more vulnerable security classification or sensitivity level.

g) The service provider must recommend to the commissioning entity that it implement probes approved by ANSSI at the appropriate level and used in accordance with their technical instructions for use. These probes must receive network traffic via TAP (*Test Access Port*) type equipment that is entirely passive and cannot be managed remotely.

h) The service provider must be able to operate probes receiving traffic via TAP (*Test Access Port*) type equipment that is entirely passive and cannot be managed remotely.

i) The events from collection sources must be centralised on one or more collectors[3] located in the enclave described in requirement IV.3.14.a).

j) The collector must make it possible to carry out an initial filtering of events in order to transmit to the analytical tools only those events that are relevant to the detection service and identified in the collection strategy.

k) The collector must be able to detect saturation and loss of communication events that would prevent it from transmitting the security events to the detection service and to delay the transmission of the events to the analysis tools if necessary. The storage capacity of the collector must be known to the service provider and the commissioning entity.

l) The service provider must have a centralised view of all the events collected, including the association of each event with the collector from which it came.

m) The events must be time-stamped as soon as they are received by the collectors. The system clocks of the collectors must be synchronised with a single time source.

n) The service provider must index all of the collected events and be able to perform searches among the collected events.

o) The service provider must be able to locate and provide any collected event whatsoever upon request by the commissioning entity.

p) The service provider must put in place a process for managing the event handling and storage capacity that enables the service provider to monitor its development and to be able to modify it as necessary.

IV.2.3. Reporting management

a) The service provider must have two information channels available for the commissioning entity:

- a reporting channel (see requirement IV.2.3.b);
- a consultation channel (see requirement IV.2.3.h);

b) The service provider must have *at a minimum* the following reporting methods available:

- email;
- short text message (SMS);
- telephone.

c) The service provider must develop, together with the commissioning entity, and implement, a security incident reporting strategy enabling it to notify the commissioning entity in the event that a security incident is detected. The reporting strategy must be reviewed with the commissioning entity at the operational committee meetings defined in section IV.4.3.

d) The reporting strategy must identify, *at a minimum*, the list of security incidents to be reported, the format, the content, the time limit, and the level of sensitivity or classification of the reports, as well as the persons to be notified, particularly with respect to the security incident and its level of severity.

e) The service provider must exercise its duty to advise the commissioning entity in the development, implementation and review of the reporting strategy. In this capacity, it must advise the commissioning entity on people to be alerted and the reporting methods.

[3] For the sake of simplicity, for the remainder of this document, it is assumed that there is only one collector.

f) The service provider must recommend to the commissioning entity that it include specific reports in the reporting strategy in the occurrence that major security incidents within its information system are detected.

g) The reports must contain only the following information: the identification number of the incident ticket and a general description of the security incident.

When not transmitted via a secure channel, the reports must not under any circumstances contain detailed information about the security incident, and especially about the collected events or the detection rules that detected the security incident, the part of the commissioning entity's information system that was affected by the security incident, or the impact of the security incident.

h) The service provider must provide the commissioning entity with access to a Web portal that enables it to view open security incident tickets, monitor their status, and view the associated ongoing actions.

i) The service provider must centralise all the reports in a report storage system.

j) The service provider must be able to provide the security incident and the events associated with the origin of a report.

k) The service provider must put in place and keep up to date a centralised and chronological record by a commissioning entity referencing all of the reports carried out for the commissioning entity.

l) The service provider must put in place a process for managing the storage capacity for the reports that enables the service provider to monitor its development and to be able to modify it in accordance with the needs of the commissioning entity.

IV.3. Information protection

IV.3.1. Information systems security policy

a) The service provider must develop a risk analysis and the associated risk treatment plan covering the full scope of the security incident detection service. The analysis and the treatment plan must be formally approved in writing by the management of the service provider.

b) The risk assessment must include a list of feared incidents within the scope of the security incident detection service. This list must include, *at a minimum*:

- intrusion attempts on the detection service's information system from one of its interconnections (see section 0IV.3.9);
- rebound attempts between commissioning entities' information systems via the detection service's information system;
- privilege escalation attempts by security incident detection service operators or administrators.
- the loss of communication with one or more of the detection service's items of equipment.

c) The service provider must review the risk assessment and the associated risk treatment plan *at a minimum* once a year and in the event of any structural changes to the detection service, particularly those concerning its hosting, infrastructure or architecture.

d) The service provider must make the risk treatment plan available to the commissioning entity upon request. The service provider must indicate to the commissioning entity the safety conditions related to the transmission and storage of the risk treatment plan.

e) The service provider must develop and implement an information systems security policy based on the risk assessment.

f) It is recommended that the service provider be certified [ISO27001] for the entirety of the scope of the security incident detection service.

IV.3.2. Levels of sensitivity or classification

a) The service provider must implement a dedicated security incident detection information system by level of sensitivity or classification.

b) The service provider must, *at a minimum*, comply with the rules established by ANSSI relating to protective measures for information systems treating sensitive unclassified defence information at the *Restricted Distribution (Diffusion Restreinte)* level [IGI_1300][II_901], particularly for information identified as sensitive in the risk assessment (see requirement IV.3.1.a).

c) The detection service's information system must be approved *at a minimum* at the level of *Restricted Distribution (Diffusion Restreinte)* for supervising the commissioning entity's information systems that are not classified.

d) The detection service's information system must be approved *at a minimum* at the same classification level as the commissioning entity's supervised information systems that are classified.

e) It is recommended that the service provider use the process described in the [HOMOLOGATION] guide for approval of the security incident detection service's information system.

IV.3.3. Territoriality of the service

a) The service provider must host and handle the data related to the security incident detection service exclusively on the national territory of France. In the event that some collection sources are located outside of the national territory of France, the events originating from these sources will be transmitted to a collector located on the national territory of France.

b) The service provider must operate the security incident detection service exclusively on the national territory of France.

IV.3.4. Audit

a) The service provider must develop an audit plan designed to verify the correct implementation of the information security and protection mechanisms for which it is responsible. This audit plan must include, *at a minimum*:

- the review of logical and physical access controls implemented to protect the devices of the detection service;
- the review of privileges and access rights to the security incident detection service. This review must include the review of administrator and operator accounts *at a minimum* once a month.

b) The service provider must review the audit plan *at a minimum* once a year and in the case of any structural changes to the detection service, particularly those concerning its hosting, infrastructure or architecture.

c) The service provider must include the list of feared security incidents (see requirement IV.3.1.b) in the audit plan in order to test these scenarios.

d) The audit plan must be comprised of the organisational audits, the physical audits, the configuration audits, the architecture audits and the penetration tests.

e) The service provider must use approved information security audit service providers (PASSI) to perform the audits. The appointed PASSI service providers and the service provider must be legally independent from each other.

f) The service provider must protect the results of the audits to, *at a minimum*, the same level of sensitivity or classification as the audited information system.

g) The service provider must update the risk treatment plan (see requirement IV.3.1.a) in order to integrate the results of the audits.

h) The service provider must communicate the results of the audits to its management team. The results of the audits must be formally approved in writing by the service provider’s management team.

IV.3.5. Physical security

a) The service provider must develop and keep up to date the list of persons authorised to access the premises hosting the security incident detection service.

b) The service provider must implement mechanisms enabling it to ensure that only authorised persons can access the premises hosting the security incident detection service.

c) The service provider must implement mechanisms enabling it to log the accesses to the premises hosting the security incident detection service.

d) The service provider must define and implement controls enabling it to ensure the confidentiality and integrity of the access logs for the premises hosting the detection service using solutions approved by ANSSI [CRYPTO_B1], [CRYPTO_B3] at the appropriate level and used in accordance with their technical instructions for use.

IV.3.6. Internal security incident detection service

a) The service provider must implement, for its own account, a security incident detection service, hereinafter referred to as the “internal security incident detection service”, dealing with the information system of the security incident detection service.

b) The service provider must comply with the requirements of section IV.3 for the internal security incident detection service, except for the requirements of IV.3.2.a) and IV.3.6.a).

c) The service provider must, on the basis of the risk assessment (see requirement IV.3.1.a) and the associated list of feared security incidents (see requirement IV.3.1.b), develop a collection strategy, an analysis strategy and a reporting strategy as part of the internal detection service.

d) The service provider must deploy one or more probes on the security incident detection service’s information system. These probes must, in particular, make it possible to monitor each of the interconnections of the security incident detection service’s information system. These probes must be collection sources for the internal security incident detection service.

e) The probes deployed by the service provider as part of the internal security incident detection service must be approved by ANSSI at the appropriate level and used in accordance with their technical instructions for use. These probes must receive network traffic input feeds via TAP (*Test Access Port*) type equipment that is entirely passive and cannot be managed remotely.

f) The service provider must develop a process for managing internal security incidents. This process must include a report to the commissioning entities upon the occurrence of a security incident on the security incident detection service. The report must specify the nature of the security incident and the measures taken by the service provider to respond to it.

g) It is recommended that the service provider put in place a crisis management process in the case of the detection of a major security incident within its detection service.

h) It is recommended that the service provider uses tools enabling it to conduct static or dynamic analysis of suspicious files.

i) If the analysis tools used by the service provider rely on resources hosted on the Internet, the service provider must perform these operations outside of the security incident detection service’s information system and after obtaining the commissioning entity’s formal written consent.

j) It is recommended that the service provider use an approved security incident response service provider (PRIS) to perform the analysis of the suspicious files. In this case, the security incident detection service provider must ensure that the scope of the approval of the security incident response service provider includes the analysis of malicious code.

IV.3.7. Partitioning of the service's information system

a) The service provider must dedicate the security incident detection service's information system to the qualified services or services which are compliant, *at a minimum*, with the requirements of section IV.3 - Information protection. All other services must be performed on an information system that is physically partitioned from the service's information system.

b) The service provider must apply ANSSI's guide to information technology hygiene [HYGIENE] to the security incident detection service's information system.

c) The service provider must partition the security incident detection service's information system into multiple trust zones into which all of the devices involved in the detection service are divided:

- a collection zone, comprising all devices involved in the event management activity, including the collectors and the event storage systems;
- an analysis zone, comprising all of the devices involved in the incident management activity, including the technical analysis tools and tools for management of the service provider's internal security incident tickets;
- a reporting zone, comprising all the devices involved in the reporting management activity, including the Web portal and the messaging system;
- one or more administrative zones, comprising all of the administrative tools and administrators' workstations;
- an operations zone, comprising the operators' workstations;
- an Internet zone, comprising the workstations that are permitted to access the Internet and that are fully isolated from the other trust zones identified above (see section IV.3.8).

d) The service provider must put in place measures to ensure the partitioning between the different trust zones, in particular by using mechanisms for filtering, authentication and access control.

e) The service provider must develop and keep up to date the reference flow matrix for the security incident detection system, together with the associated filtering policy, authorising only those flows that are strictly necessary for the operation of the security incident detection service.

f) The service provider must implement IP encryption and authentication solutions between these trust zones as soon as the information exchanged between these zones passes through transport networks that are not dedicated to the detection service. These IP encryption and authentication solutions must be approved by ANSSI at the appropriate level and used in accordance with their technical instructions for use.

g) The service provider must develop and keep up to date a detailed description of the architecture of the security incident detection service's information system. This description must identify all of the information system's devices and the trust zones of the detection service.

h) The service provider must partition between the commissioning entities:

- the storage and event handling systems;
- the security incident storage and handling systems, the technical analysis tools and the security incident ticket management tools;
- the reports, the Web portal and the messaging system.

This partitioning must be achieved through logical access control mechanisms *at a minimum*, and implemented in accordance with the specific operational requirements (rights, privileges, authentication, etc.).

IV.3.8. Administration and operation of the service

a) The administrators must manage the security incident detection service’s devices through dedicated administrative workstations, hosted in the administration zone[4] and separated from the operator workstations.

b) The administration of the security incident detection service’s devices must be possible only from the administration zone via the network interfaces of the devices dedicated to administration.

c) The service provider must log each access to the security incident detection service’s devices and the actions performed.

d) The service provider must put in place a centralised administration directory that is dedicated to the authentication of administrators. This directory must be deployed in the administration zone.

e) The service provider must put in place a centralised operation directory that is dedicated to the detection service that enables, in particular, the authentication on all of the detection service’s devices and the opening of sessions on operator workstations.

f) The service provider must put in place measures to ensure that administrators manage the security incident detection service’s devices using administrative accounts dedicated to these tasks and accessible only to administrators.

g) The administrators must not have administrative rights on their administration workstations.

h) The service provider must implement controls to ensure that the administrators and operators can access only those resources that are relevant to their tasks (see Annex 2).

i) The service provider must apply controls depriving operators of administrative rights on the detection service’s devices, including on their own workstations.

j) The workstations of administrators and operators must be connected exclusively to the security incident detection information system.

In the event of a need to access the Internet or other information systems (the service provider’s internal information system, for example), administrators and operators must have a separate workstation that is distinct from their normal workstation and that is not connected to the security incident detection service’s information system.

k) The service provider must put in place an exchange zone for transferring files from outside of the information system as part of the administration or operation of the detection service. This exchange zone must be distinct and independent between administrators and operators. The service provider must meet the requirements for the exchange zone set out in the “Exchange system” *(“Système d’échange”)* section of the [NT_ADMIN] technical note.

l) All exchanges related to the detection service from administration or operations workstations must be performed using encryption and authentication protocols that comply with ANSSI requirements[CRYPTO_B1],[CRYPTO_B3].

[4] It is recommended that the ANSSI technical note regarding the secure administration of information systems [NT_ADMIN] be followed.

IV.3.9. Interconnections with the service's information system

a) The only authorised interconnections with the security incident detection service are those with:

- the commissioning entity's information system:
    - for the collection of events,
    - for the administration of collection devices[5],
    - for the operation of collection devices[6],
    - for reporting security incidents.
- the remote administration and operation workstations (see IV.3.10) via specific gateways;
- the update servers for downloading updates of security incident detection service devices via a relay station (see IV.3.11);
- the exchange zone for the transfer of files from the Internet.

b) The service provider must filter flows at all interconnections with the security incident detection service's information system using filtering solutions approved by ANSSI at the appropriate level and used in accordance with their technical instructions for use.

c) The interconnections with the security incident detection service, particularly those using a transport network other than that of the security incident detection service must be encrypted using IPsec encryption and authentication solutions approved by ANSSI at the appropriate level and used in accordance with their technical instructions for use.

d) The equipment used for the encryption and authentication of interconnections must be dedicated to the qualified security incident detection service.

e) The service provider must protect the confidentiality, integrity and authenticity of all information exchanged between the security incident detection service's information system and the commissioning entity's information system using solutions approved by ANSSI [CRYPTO_B1], [CRYPTO_B3] at the appropriate level and used in accordance with their technical instructions for use.

IV.3.10. Remote access

a) In the case of remote access to the security incident detection service, the service provider must put in place an administration gateway and an operations gateway.[7]

b) The remote workstations used must be dedicated to the approved services and to any service that is compliant with the requirements of section IV.3 - Information protection.

c) The administration flow between remote administration workstations and the detection service's information system must transit via a dedicated administration gateway.

d) The operation flow between remote operations workstations and the detection service's information system must transit via a dedicated operations gateway.

[5] Only if the commissioning entity authorises the service provider to manage one or more devices hosted in this zone (see requirement IV.3.14.k).

[6] Only if the commissioning entity authorises the service provider to operate one or more devices hosted in this zone (see requirement IV.3.14.k).

[7] In compliance with the technical note [NT_ADMIN].

e) The administration gateway and the operations gateway must be separated. In the event that part of the administration or operation is subcontracted, provision must be made for physical gateways that are separated from the administration and operations gateways.

f) The flows between remote workstations and gateways must be encrypted using IPsec encryption and authentication solutions approved by ANSSI at the appropriate level and used in accordance with their technical instructions for use.

g) The administrators and operators must authenticate with *a minimum of* two factors.

h) It is recommended that, for remote access, the service provider implement an authentication process based on digital certificates issued by electronic certificate service providers approved by ANSSI at a RGS *** level and therefore involving the use of cryptographic media approved by ANSSI at an enhanced level.

i) Remote workstations must be hardened, configured so that they are able to communicate exclusively with the dedicated remote access gateway, permit only the use of removable media that is authorised by the information systems security policy, and have their entire disks encrypted with an encryption solution approved by ANSSI at the appropriate level.

j) The service provider must configure the filtering solutions (see requirement IV.3.7.d) so that they only allow flows initiated from the remote workstations.

IV.3.11. Relay station for updating the service's devices

a) The service provider can implement an internal relay station connected to a dedicated Internet gateway to enable the downloading of updates of the security incident detection service's devices.

b) The service provider must conduct a manual, offline update of the security incident detection service's devices that cannot be updated via a relay station.

The following requirements apply when a relay station has been put in place.

c) The service provider must implement a whitelist filter to ensure that the relay station will only download official updates for the security incident detection service's devices from the vendor's official update sources.

d) It is recommended that the service provider ensure the authenticity and integrity of downloaded updates from authorised update sources.

e) The service provider must configure the filtering solutions (see requirement IV.3.7.d) so that they only allow flows initiated from the relay station to the Internet.

IV.3.12. Web portal and reporting tools

a) The service provider must put in place a directory dedicated to the authentication of the commissioning entity on the Web portal. The service provider must authenticate the commissioning entity using *a minimum of* two factors in order to access the Web portal. The service provider must maintain a list of persons who are authorised to access the Web portal, together with their associated privileges.

b) It is recommended that the service provider implement an authentication process for the Web portal based on digital certificates issued by electronic certificate service providers approved by ANSSI at a RGS *** level and therefore involving the use of cryptographic median approved by ANSSI at an enhanced level.

c) The service provider must implement a Web application firewall to filter queries to the Web portal.

d) The service provider must implement security controls on the messaging systems used for reporting management (attachment filtering, virus scanning, restrictions on the size of attachments, etc.).

IV.3.13. Backups

a) The service provider must develop and implement a backup and restoration plan for the security incident detection service's devices. The backup plan must include several distinct components, including *at a minimum* the following components:

- system backups;
- configuration backups;
- data backups.

b) The service provider must test the backup and restoration plan once a year *at a minimum*.

c) The service provider must define and implement controls to ensure the confidentiality and integrity of the backups performed. The backup device must be dedicated and located in an administration zone that provides for the partitioning of the backup activities, in compliance with the backup plan.

d) It is recommended that the service provider complies with all of the controls and recommendations regarding securing backups of [ISO27002].

IV.3.14. Security of the enclave within the commissioning entity's information system

a) The entire security incident detection service's devices deployed in the commissioning entity (in particular, the collectors) must be positioned within one or more enclaves[8] within the commissioning entity's internal information system.

b) The enclave must host only those devices that make it possible to ensure the provision of the security incident detection service.

c) The enclave must follow the rules established in the ANSSI information technology hygiene guide [HYGIENE].

d) It is recommended that the requirements of section IV.3.2 covering the protection of information within the service provider's security incident detection service be applied to this enclave.

e) The partitioning of the enclave must be performed by:

- a filtering device between the enclave and the commissioning entity's internal information system;
- a filtering device between the enclave and the service provider's security incident detection service.

f) The filtering device between the enclave and the commissioning entity's internal information system must block all flows except those initiated from the commissioning entity's internal information system to this zone and enabling the collection sources hosted on the commissioning entity's internal information system to transmit the events to this zone.

g) The collection sources must be the only devices authorised to send information to the collectors, and such collectors must be configured exclusively in listening mode. No flow may be initiated from the collectors to the collection sources.

h) It is recommended that an intermediate collector be implemented under the responsibility of the commissioning entity when the collection sources cannot transmit the events directly to the collectors in the collection zone.

i) The service provider must not under any circumstances have rights on the filtering device between this enclave and the commissioning entity's internal information system (see requirement IV.3.14.e).

[8] For the sake of simplicity, for the remainder of this document it is assumed that there is only one enclave.

j) The filtering device between this enclave and the information system of the service provider's security incident detection service must block all flows except:

  - those initiated from this enclave to the information system of the service provider's security incident detection service and that only enable the transmission of the events from this enclave to the information system of the service provider's security incident detection service. The service provider must limit as much as possible the number of flows that permit the events of this enclave to be transmitted to the security incident detection service's information system;
  - those enabling the service provider to manage from the administration zone, the devices hosted in that zone (see requirement IV.3.7.c)[9];
  - those permitting the service provider to operate from the operation zone (see requirement IV.3.7.c), the devices hosted in that zone.[10]

k) The service provider must define in the service agreement, together with the commissioning entity, the responsibilities applicable to the administration and operation of the devices hosted in this enclave, including:

  - the security incident detection devices (sensors, collectors, etc.);
  - the filtering devices[11] that ensure the partitioning of this enclave (see requirement IV.3.14.e);
  - the devices that make it possible to protect the confidentiality and authenticity of the information exchanged between the enclave and the security incident detection service's information system.

l) The service provider must be able to fully ensure the performance of its security incident detection service without having rights on the devices hosted within this enclave.

m) It is nevertheless recommended that the service provider have the responsibility for the administration and operation of security incident detection devices hosted within this enclave and that the commissioning entity have the responsibility for the other devices (see requirement IV.3.14.k).

n) The service provider must apply the recommendations set out in the ANSSI technical note on the implementation of a logging system [NT_JOURNAL] when the devices are deployed in the enclave under its responsibility[12].

IV.4. Organisation of the service provider and governance

IV.4.1. Code of ethics and recruitment

a) The service provider must verify the training, qualifications, and employment references of candidates for the detection service and the truthfulness of their curriculum vitae prior to hiring them.

b) The service provider must require applicants to provide proof that they do not have a criminal record *("bulletin n° 3 du casier judiciaire").*

[9] Only if the commissioning entity has authorised the service provider to manage one or more devices hosted in this enclave (see requirement IV.3.14.k).

[10] Only if the commissioning entity has authorised the service provider to operate one or more devices hosted in this enclave (see requirement IV.3.14.k).

[11] With the exception of the filtering device that ensures the partitioning between this enclave and the commissioning entity's internal information system (see requirement IV.3.14.e)

[12] The responsibilities for this zone are defined in the service agreement in compliance with requirement IV.5.3.3.a)

c) The operators, administrators and specialists in the detection service must have a contractual relationship with the service provider or one of its subcontractors in the event the service provider subcontracts part of its activities.

d) The service provider must have a code of ethics incorporated into its internal regulations, stipulating, in particular, that:

- the services are performed with loyalty, discretion and impartiality;
- employees use only those methods, tools and techniques that have been approved by the service provider;
- employees undertake to not disclose information to a third party, even if anonymised and decontextualized, which has been obtained or generated as part of the service, without the commissioning entity’s formal written authorisation;
- employees undertake to alert the service provider to all clearly illegal content discovered during the provision of the service;
- employees undertake to comply with the national legislation and regulations in force and with best practices related to their activities.

e) The service provider must ensure that all of its employees sign the code of ethics referred to in the previous requirement prior to performing the service.

f) The service provider must ensure the compliance with the code of ethics and makes provision for disciplinary sanctions for operators, administrators and experts of the detection service who have breached the security rules or the code of ethics.

g) The service provider must develop and implement a plan for raising the awareness of its employees with respect to information system security and the security measures associated with it, as well as to the national legislation and regulations in force relating to the security incident detection service.

IV.4.2. Organisation and management of competencies

a) The service provider must have a team that:

- ensures the performance of, *at a minimum*, the tasks described in Annex 2;
- has the skills associated with these tasks.

b) The service provider must employ a sufficient number of employees and may use subcontracting (see section IV.5.3.7 entitled “Subcontracting”) to ensure that the service provided is a qualified service in all respects.

c) The service provider must develop and implement a training plan designed for the use of the detection service team and which is adapted to its tasks.

d) The service provider must develop and make available to employees guides about the operation and administration of the security incident detection service’s devices.

e) It is recommended that the service provider put in place an on-call system enabling it to mobilise a part of its team outside working hours.

f) The service provider must have within its service a watch centre for cyber-attack or must subscribe to such a service.

g) It is recommended that the watch centre for cyber-attack be referenced by the French national CERT.

h) The service provider must provide the commissioning entity with a remote support service that allows in particular:

- the commissioning entity to declare a suspected or confirmed security incident to the service provider;

- the service provider to help the commissioning entity to resolve production problems related to the devices managed by the service provider;
- the service provider to assist and advise the commissioning entity.

i) The service provider must make the support service accessible via a telephone number or email address.

j) The service provider must implement mechanisms enabling it to exchange information with the commissioning entity *at a minimum* at the *Restricted Distribution (Diffusion Restreinte)* level via the support service.

k) The service provider must appoint a person to serve as an operational point of contact for the commissioning entity. This person is the main contact point with respect to the operational functioning of the security incident detection service and the monitoring of detected security incidents. The service provider must inform the commissioning entity of any change to the person serving as the operational point of contact for the security incident detection service.

l) It is recommended that the commissioning entity appoint a person to serve as an operational point of contact for the security incident detection service.

m) The persons serving as operational points of contacts must participate in the operational and strategic committee meetings defined in section IV.4.3.

IV.4.3. Operational and strategic committees

IV.4.3.1. Operational committee

a) The service provider must put in place and chair an operational committee meeting, in the presence of the commissioning entity, once per quarter *at a minimum.*

b) It is recommended that the service provider hold an operational committee meeting once a month.

c) The operational committee must discuss, *at a minimum,* the following topics:

- an overall assessment of the security incident detection service:
  - a review of the operational indicators (see section IV.5.1);
  - a review of the detected security incidents;
  - a review of the collection, analysis and reporting strategies;
  - a review of the list of detection rules (see requirement IV.2.1.h);
  - a review of the detection rule status updates (see requirement IV.2.1.i).
- the scope of the security incident detection service:
  - a review of the commissioning entity’s context;
  - a review of changes affecting the commissioning entity’s information system;
  - a presentation of the evolution of any projects impacting the scope of the service;
  - a review of the list of feared security incidents.
- possible improvements to the security incident detection service:
  - a review of the quality indicators (see section IV.5.1);
  - an analysis of the operational evolutions in the security incident detection service (evolution of tools, modifications of operational processes, etc.);
  - a presentation of the detection rules that have been created, modified or withdrawn;
  - a presentation of the detection rules that have not been triggered for a period of one year.

d) The service provider must write a report after each operational committee meeting and send it to the commissioning entity for approval. This report must contain *at a minimum* the list of the participants, the decisions taken at the committee meeting and the associated action plan.

IV.4.3.2. Strategy committee

a) The service provider must put in place and chair a strategy committee meeting, in the presence of representatives from the service provider’s senior management team, *at a minimum* once a year.

b) It is recommended that the service provider hold a strategic committee meeting twice a year.

c) The strategy committee must address *at a minimum* the following topics:

- a review of the strategic indicators (see section IV.5.1);
- a review of the service agreement;
- a review of the reversibility plan;
- a summary presentation of the effectiveness of the detection service;
- a review and predictions of threats.

d) The service provider must write a report after each strategy committee meeting and send it to the commissioning entity for approval. This report must contain *at a minimum* the list of the participants and the decisions taken at the committee meeting.

IV.5. Quality and level of service

IV.5.1. Quality of service

a) It is recommended that the service provider be [ISO9001] certified in respect of the scope of the security incident detection service.

b) The service provider must develop and implement a knowledge capitalisation process for the detected security incidents in order to continually improve the effectiveness of its detection service.

c) The service provider must define, with the commissioning entity, the operational and strategic indicators for the security incident detection service.

d) It is recommended that the service provider use the indicators proposed in [ETSI_ISG_ISI].

e) The service provider must put in place, *at a minimum*, the following operational activity indicators:

- incident management:
    - the number of incidents detected per month;
    - the number of confirmed incidents following a qualification per month;
    - the number of detection rules implemented in the technical analysis tools;
    - the number of detection rules created, modified or withdrawn per month, by origin (monitoring activity, requested by the commissioning entity, etc.);
    - the availability rate of the technical analysis tools;
    - the number of detection rules triggered per month;
    - the fill rate of the incident storage systems;
    - the remaining capacity of the incident storage systems;
    - the list of detection rules that have never been triggered.
- event management:

    - the number of collection sources;
    - the number of collectors;
    - the number of events collected per day / per month;
    - the number of events collected by collector per day / per month;
    - the number of events sent to the technical analysis tools per day / per month;
    - the fill rate of each of the event storage systems, including the collectors in the enclave if they are under the responsibility of the service provider;
    - the remaining capacity of each of the event storage systems, including the collectors in the enclave if they are under the responsibility of the service provider.
  - reporting management:
    - the availability rate of the Web portal;
    - the availability rate of the messaging server;
    - the number of reports sent to the commissioning entity per month, by level of severity of the security incident;
    - the number of security incident tickets opened per month;
    - the number of security incident tickets closed per month;
    - the minimum / average / maximum time between creating and closing a ticket;
    - the number of accounts authorised to access the Web portal;
    - the number of Web portal access accounts created per month;
    - the number of Web portal access accounts deleted per month;
    - the number of successful Web portal authentications per month;
    - the number of failed Web portal authentications per month.

f) The service provider must put in place, *at a minimum*, the following operational effectiveness indicators:

  - incident management:
    - the maximum time taken to qualify an incident;
    - the average time taken to qualify a security incident according to its level of severity;
    - the average time taken to update the detection rules following a request by the commissioning entity;
    - the average time taken to search for a single incident;
    - the number of incident qualification errors;
    - the incident qualification error rate;
    - the number of events not recognised and therefore not taken into account by the technical analysis tools;
    - the rate of events not recognised and therefore not taken into account by the technical analysis tools.
  - event management:
    - the minimum / average / maximum time between the generation of an event by the collection source and its storage in the event storage systems;

        - the minimum / average / maximum time between the generation of an event by the collection source and it being sent to the technical analysis tools;
        - the minimum / average / maximum time taken to process the search for an event in the event storage systems;
        - the availability rate of each event management device, including the collectors in the enclave if they are under the responsibility of the service provider.
    - reporting management:
        - the minimum / average / maximum time between the detection and the reporting of a security incident, by level of severity;
        - the number of erroneous reports (false positives, etc.).

g) The service provider must put in place, *at a minimum*, the following strategic indicators:

- the consolidation of the operational indicators;
- the availability rate of the detection service;
- the availability rate of the detection service’s technical devices;
- the number of confirmed incidents found on the service provider’s information system per month within the scope of the commissioning entity’s detection service;
- the rate of compliance with the level of quality required by commissioning entity.

h) The service provider must establish and keep up to date a process for measuring the indicators which describes, for each of the described operational and strategic indicators, the methods and means used by the service provider to measure the indicator.

IV.5.2. Reversibility

a) The service provider must develop, with the commissioning entity, a reversibility plan for the security incident detection service enabling the restoration of service by the commissioning entity or another service provider.

b) The reversibility plan must contain, *at a minimum*, the following elements:

- a comprehensive inventory of the information and material to be restored;
- the duration of the reversibility;
- the people involved and the actions that each of them is required to perform;
- the formats of the information to be restored;
- the means of restoration.

The service provider must be able, if the commissioning entity so requests, to restore the stored security events, together with the specific detection rules, to the commissioning entity of the service.

c) The duration of the reversibility must be *at a minimum of* three months.

d) It is recommended that the duration of the reversibility be six months.

e) The service provider must maintain the security incident detection service in operational condition during the implementation of the reversibility plan.

f) The service provider must destroy all information relating to the commissioning entity at the end of the execution of the reversibility plan, with the exception of information that the commissioning entity has authorised it to retain (see requirement IV.5.3.4.a).

IV.5.3. Service agreement

IV.5.3.1. Terms of delivery of the service

a) The service agreement must:

- describe the scope and objectives of the service to be provided, the security incident detection service, including in particular the event, incident, and reporting management activities;
- describe the technical and organisational measures implemented by the service provider as part of the performance of the service;
- define the deliverables expected as part of the performance of the service, the intended recipients, and their level of sensitivity or classification, together with the associated modalities;
- describe the methods of communication between the service provider and the commissioning entity that will be used in providing the service;
- define the rules of ownership of the elements protected by intellectual property, such as the deliverables, the tools and the detection rules specifically developed by the service provider as part of the provision of the service;
- describe the process of registering and handling complaints by the commissioning entity, the victim or third parties, as well as the procedures for filing a complaint;

IV.5.3.2. Organisation of the service

a) The service agreement must:

- stipulate that the service provider appoint a contact person for the commissioning entity, who will be in charge of ensuring the operational monitoring of the service;
- stipulate that the service provider and the commissioning entity specify the names, roles, responsibilities, rights and need to know of the individuals involved in the provision of the service. This clause is particularly important if there is a security incident that must not be made public;
- stipulate that the service provider collaborate with third parties mandated by the commissioning entity and specifically appointed by the latter. This clause must, in particular, enable the service provider to work with a security incident response service provider mandated by the commissioning entity in the event of a suspected or confirmed security incident;
- stipulate that the service provider does not involve employees who do not have a contractual relationship with it, did not sign the code of ethics or who have a criminal record;
- stipulate whether the service provider allows remote access by administrators or operators to the security incident detection service's information system.

IV.5.3.3. Responsibilities

a) The service agreement must:

- stipulate that the service provider do not provide the service until receiving formal written approval of the service agreement by the commissioning entity;
- stipulate that the service provider inform the commissioning entity in the event of any deficiency in the service agreement;
- stipulate that the service provider inform the commissioning entity in the event that a security incident is detected on the security incident detection service's information system, and the maximum time permitted to transmit the information following an incident;

- stipulate that the service provider perform only those actions that are strictly in line with the objectives of the service;
- stipulate that the commissioning entity possess all of the ownership rights and access rights required for the scope of the service (information systems, physical media, etc.) or that it has obtained the agreement of any third party, including its service providers or partners, whose information systems are included within the scope of the service;
- stipulate that the commissioning entity meet all of the legal requirements necessary for the service and in particular those relating to the collection and analysis of information;
- define the responsibilities and the precautions to be observed by all parties regarding the potential risks related to the service, especially with regard to the confidentiality of the information collected and analysed and the availability and integrity of the commissioning entity's information system;
- stipulate that the service provider have professional liability insurance covering any damage caused to the commissioning entity and in particular to its information system as a result of its service, specifying the coverage of the insurance and including the insurance certificate;
- define the responsibilities between the service provider and the commissioning entity with respect to the enclave of the security incident detection service within the commissioning entity's information system (see section IV.3.14). Requirements IV.3.14.k) to IV.3.14.m) make it possible to help the service provider and the commissioning entity to define these responsibilities;
- stipulate that the service provider have in place a change management procedure for its own information system;
- stipulate that the service provider have in place a process for the continuous improvement of the effectiveness of its detection service, based on, in particular, the operational indicators set out in section IV.5.1.

IV.5.3.4. Confidentiality and information protection

a) The service agreement must:

- identify the level of sensitivity or classification of the security incident detection service implemented by the service provider;
- identify the level of sensitivity or classification of the commissioning entity's information system concerned by the agreement;
- stipulate that the service provider only collect and analyse the information that is strictly required for the smooth operation of the service;
- stipulate that the service provider not disclose any information relating to the service to third parties without the formal written authorisation of the commissioning entity;
- specify the clauses relating to the ethical requirements of the service provider and include the service provider's code of ethics;
- specify the terms of access, storage, transmission, reproduction, destruction and restoration of the information and materials collected and analysed by the service provider. If necessary, the service provider must define the terms, in collaboration with the commissioning entity, in accordance with the types of information or the physical media on which it is stored;
- stipulate that the service provider may, except in the case of a formal written refusal by the commissioning entity, retain certain types of information related to the service, and that it specifies these types of information (e.g. detection rules, malware, attack scenarios, indicators of compromise, etc.);

- stipulate that the service provider anonymise and decontextualize (deleting any information that could be used to identify the commissioning entity, any information of a personal nature, etc.) all of the information that the commissioning entity authorises it to retain;
- stipulate that the service provider immediately destroy all information related to the service on the expiry date of the retention period;
- stipulate that the service provider destroy all information about the commissioning entity at the end of the service, with the exception of information that the commissioning entity has authorised it to retain;
- stipulate that the service provider, except in the event of written formal refusal by the commissioning entity, transmit to the French national CERT the anonymised and decontextualized information, together with their level of sensitivity and their conditions of use;
- define the frequency with which the service provider shall test the backup and restoration plan of the security incident detection service.

IV.5.3.5. Reversibility

a) The service agreement must specify the terms of implementing a reversibility plan for the service: duration, implementation, any additional costs, etc. (see section IV.5.2)

IV.5.3.6. Laws and regulations

a) The service agreement must:

- be written in French. The service provider must provide a courtesy translation of the service agreement if the commissioning entity requests it;
- stipulate that the French version shall prevail, particularly in the context of a legal dispute;
- stipulate that the governing law for the service agreement is French law;
- specify the technical and organisational measures implemented by the service provider in order to comply with French legislation, in particular those concerning:
  - personal data [LOI_IL];
  - professional secrecy [CP_ART_226-13], without prejudice to the application of article 40, paragraph 2 of the Code of Criminal Procedure relating to reporting to a judicial authority;
  - breach of trust [CP_ART_314-1];
  - confidentiality of private correspondence [CP_ART_226-15];
  - medical confidentiality [CSP_ART_L1110-4];
  - invasion of privacy [CP_ART_226-1];
  - fraudulent access to or maintenance in an information system [CP_ART_323-1];
- specify any specific regulatory and legal requirements to which the commissioning entity is subject and, in particular, those relating to its sector of activity;
- establish the requirements to be met by the service provider in the context of judicial, civil or arbitration proceedings;
- define the retention period for information related to the service, and in particular for the collected events and the detected security incidents. If necessary, distinctions in retention periods may be made based on the different types of information. The minimum retention period is six months, in accordance with French legislation and regulations.

IV.5.3.7. Subcontracting

a) The service agreement must specify that the service provider may subcontract all or part of the service to another service provider who is qualified to perform the outsourced activities, provided that:

- there is a service agreement between the service provider and the subcontractor;
- the use of subcontracting is known to, and has been formally accepted in writing by, the commissioning entity.

IV.5.3.8. Deliverables

a) The service agreement must specify that the deliverables of the service shall be in French, except at the formal written request of the commissioning entity.

IV.5.3.9. Approval of the service

a) The service agreement must state that:

- the service provided is an approved service and must include the service provider's proof of approval;
- in accordance with the approval process for trust service providers [PROCESS_QUALIF], the commissioning entity may file a claim against the service provider to ANSSI;
- in accordance with the approval process for trust service providers [PROCESS_QUALIF], the commissioning entity authorises ANSSI and the approval entity to audit the information system of the service provider's security incident detection service.
- in accordance with this reference document (see requirement IV.3.4.e), the commissioning entity authorises an approved audit service provider for information system security (PASSI) to audit the information system of the service provider's security incident detection service as part of the audit plan.

IV.5.3.10. Service level

a) The service agreement must:

- define the operational and strategic indicators used to measure the service level of the service;
- define the operating hours for the security incident detection service;
- stipulate that the service provider shall hold operational and strategic committee meetings in the presence of the commissioning entity;
- specify the objectives and the frequency of these committee meetings;
- identify, for the service provider and the commissioning entity, the level of human resources dedicated to managing the detection rules and, in particular, their creation and modification;
- define the frequency with which the service provider transmits the detection rule status report to the commissioning entity;
- stipulate that the service provider shall make a support service available to the commissioning entity and the hours during which this support service will be in operation;
- specify the type of support service (phone, email, etc.), its availability, and the level of sensitivity or classification of information that can be exchanged;
- specify the level of competence of the employees who are on call, in accordance with the needs of the commissioning entity and in the event that on-call services are put in place.

Annex 1 Documentary references

I. Codes, laws and regulations

Reference	**Document**
[LOI_IL]	Law of 6 January 1978 on information technology, data files and civil liberties. Available on http://www.legifrance.gouv.fr.
[CP_ART_314-1]	Article 334-1 of the French penal code on the abuse of trust.
[CP_ART_226-1]	Article 226-1 of the French penal code on the invasion of privacy.
[CP_ART_226-13]	Article 226-13 of the French penal code concerning professional secrecy.
[CP_ART_226-15]	Article 226-15 of the French penal code relating to confidentiality of correspondence.
[CP_ART_323-1]	Article 323-1 of the French penal code on access or fraudulent maintenance in an automated data processing system.
[CSP_ART_L1110-4]	Article L1110-4 of the French public health code relating to medical confidentiality.
[IGI_1300]	French interministerial general instruction n° 1300 on the protection of the secrets of national defence, n°1300 /SGDSN/PSE/PSD, 30 November 2011. Available on http://www.legifrance.gouv.fr.
[II_910]	French interministerial instruction on controlled items of information system security (ACSSI), n°910/SGDSN/ANSSI, 22 October 2013. Available on http://www.legifrance.gouv.fr.
[II_901]	Interministerial instruction on the protection of sensitive information systems, n°901/SGDSN/ANSSI, 28 January 2015. Available on http://www.legifrance.gouv.fr.

II. Standards and technical documents

Reference	**Document**
[PDIS_LPM]	Additional requirements applicable to service providers of security incident detection services under law n° 2013-1168 of 18 December 2013. This document is marked *Diffusion Restreinte* and can be obtained from ANSSI.
[CRYPTO_B1]	Rules and recommendations concerning the choice and size parameters of cryptographic mechanisms, ANSSI, version 2.03. Available on http://www.ssi.gouv.fr.
[CRYPTO_B3]	Rules and recommendations concerning authentication mechanisms, ANSSI. Available on http://www.ssi.gouv.fr.
[HOMOLOGATION]	Security accreditation in nine simple steps, ANSSI, current version. Available on http://www.ssi.gouv.fr.
[HYGIENE]	Guide to Information Technology Hygiene, ANSSI, current version. Available on http://www.ssi.gouv.fr.
[NT_JOURNAL]	Security recommendations for the implementation of a logging system, technical note n° DAT-NT-012/ANSSI/SDE/NP of 2 December 2013, ANSSI. Available on http://www.ssi.gouv.fr.
[NT_ADMIN]	Recommendations on the secure administration of information systems, technical note n° No DAT-NT-22/ANSSI/SDE/NP of 20 February 2015, ANSSI Available on http://www.ssi.gouv.fr.

Reference	**Document**
[ETSI_ISG_ISI]	ETSI ISI Indicator standards (ISI 001-1 and Guides 001-2), ISI Event Model (ISI-002), ISI Maturity (ISI-003), ISI Event Detection (ISI-004) – 5 standards on security incident detection.
[ISO9001]	International standard ISO 9001:2008: Quality management systems – Requirements. Available on http://www.iso.org.
[ISO27000]	International standard ISO/IEC 27000:2014: Information technology – Security techniques – Information security management systems – Overview and vocabulary. Available on http://www.iso.org.
[ISO27001]	International standard ISO/IEC 27001:2013: Information technology – Security techniques – Information security management systems – Requirements. Available on http://www.iso.org.
[ISO27002]	International standard ISO/IEC 27002:2013: Information technology – Security techniques – Code of best practice for information security management. Available on http://www.iso.org.
[ISO27005]	International standard ISO/IEC 27005:2011 – Information technology – Security techniques – Managing risks related to information security. Available on http://www.iso.org.
[ISO27035]	International standard ISO/IEC 27035:2011: Information technology – Security techniques – Managing information security incidents. Available on http://www.iso.org.

III. Other documentary references

Reference	**Document**
[STRAT_NUM]	National digital security strategy, October 2015. Available on http://www.ssi.gouv.fr
[PROCESS_QUALIF]	Approval process for a trust service provider, current version. Available on http://www.ssi.gouv.fr
[GUIDE_ACHAT]	Buyer’s guide to security products and qualified trust services, current version. Available on http://www.ssi.gouv.fr

Annex 2 Tasks and skills of the service provider's employees

I. Operation

I.1. Tasks

- identifying and qualifying the security incidents;
- supporting the investigation teams in handling the incidents.

I.2. Skills

- knowledge of protocols and network architectures;
- log analysis experience (systems or applications);
- knowledge of information systems security;
- network traffic analysis skills;
- detection service devices knowledge, including searching for events in the event storage systems.

II. Administration

II.1.Tasks

- managing the devices of the security incident detection service;
- maintaining the devices of the security detection service in operational conditions;
- updating the devices of the security incident detection service.

II.2.Skills

- security incident detection service devices knowledge, particularly related to event, incident and reporting management.

III. Detection

III.1. Tasks

- designing and maintaining an architecture for the detection service;
- integrating or developing and maintaining the components of the detection service;
- integrating or developing and maintaining new correlation engines.

III.2. Skills

- operation of probes and event log correlation tools knowledge;
- mastery of common protocols for the operation of the services;
- good knowledge of the most common applications and their security (web servers, mail servers, database servers, DNS servers, proxies, firewalls, etc.);
- good knowledge of the global network architecture and the security of its components (routers, switches, etc.).

IV. Collection and log analysis

IV.1. Tasks

- contributing to defining and reviewing the collection strategy;
- contributing to defining the commissioning entity's logging policy by type of equipment (operating systems, infrastructure services, network equipment, security equipment, etc.);
- providing support to administrators in the deployment of detection systems (tests, maintaining the systems in operational condition, support for analysts using these systems, etc.);
- participating in the development and maintenance of event correlation mechanisms and rules.

IV.2. Skills

- in-depth knowledge of system, network and applications event log analysis;
- knowledge of event log correlation tools and techniques;
- knowledge of log analysis or security monitoring systems (security information and event management – SIEM).

V. Detection rule management

V.1. Tasks

- expanding internal knowledge bases with information on threats, vulnerabilities and malicious code;
- creating, improving and disabling detection rules;
- ensuring the continuous improvement of the reporting process.

V.2. Skills

- knowledge of vulnerabilities;
- knowledge of command and control protocols;
- knowledge of operational modes of attacks and malicious codes;
- expertise in detection rules development tools.

Annex 3 Recommendations for commissioning entities

This annex lists ANSSI's recommendations for commissioning entities in relation to security incident detection services.

I. Approval

a) The commissioning entity may, when it is an administrative authority or an operator of vital importance, ask ANSSI to participate in defining the specifications covered by a tender or contract.

b) It is recommended that the commissioning entity choose its service provider from among those listed in the catalogue of approved service providers published on ANSSI's website: the approval of a security incident detection service provider demonstrates its compliance with all of the requirements of this reference document.

c) To receive the benefits of an approved service, i.e. one that complies with all of the requirements of this reference document, the commissioning entity must:

- select the service provider from among those listed in the catalogue of approved service providers published on ANSSI's website;
- require the service provider to stipulate in the service agreement that the service provided is an approved service.

Approved service providers retain the ability to provide non-approved services. Using a service provider from among those listed in the catalogue of approved service providers is therefore a necessary condition but not a sufficient one for receiving an approved service: the commissioning entity must also require an approved service.

d) It is recommended that the commissioning entity use the buyer's guide to security products and trust services [GUIDE_ACHAT], the purpose of which is to assist commissioning entities in making buying decisions during the tender process.

e) It is recommended that the commissioning entity ask the service provider to submit its proof of approval. This certificate identifies, in particular, the activities for which the service provider is approved and the expiry date of the approval.

f) In accordance with the approval process for trust service providers [PROCESS_QUALIF], the commissioning entity may file a complaint with ANSSI against an approved service provider if it considers that the service provider has not met one or more of the requirements of this reference document in providing an approved service.

If, following investigation of the complaint, it is determined that the service provider has not complied with one or more of the requirements of this reference document in providing an approved service, and depending on the severity of such breach, the service provider's approval may be suspended or revoked, or the scope of its approval may be reduced.

g) Approval of a service provider does not attest to its capacity to access or hold classified information [IGI_1300] and is therefore not a substitute for a clearance.

It is possible for a commissioning entity to use an approved service provider after ensuring that it has adequate clearances if necessary.

h) Approval of a service provider does not attest to its capacity to access or hold controlled items of information system security (ACSSI) [II_910].

It is possible for a commissioning entity to use an approved service provider after ensuring that the latter has, *at a minimum*, for service providers with ACSSI clearance, adequate ACSSI access clearance (DACSSI), or, for service providers without ACSSI clearance, certificates of ACSSI manipulation training.

II. Before the start of the service

a) It is recommended that the commissioning entity appoint a person to serve as an internal operational point of contact responsible for being the main point of contact with the service provider with respect to the operational functioning of the security incident detection service and for monitoring the detected security incidents.

b) It is recommended that the commissioning entity retain an approved audit service provider for information system security (PASSI)[13] to draw up the risk assessment for establishing the list of feared security incidents and associated impacts (see requirement IV.2.1.a) from which the collection, analysis and reporting strategies are developed.

c) It is recommended that the commissioning entity update its risk assessment each time that there is a change in its infrastructure or its services, and that it communicate these changes and their consequences to the service provider.

d) It is recommended that the commissioning entity identify in the service agreement any specific legal and regulatory requirements to which it is subject, including those related to its sector of activity.

e) It is recommended that the commissioning entity require to the service provider that the frequency of the operational committee meetings (see section IV.4.3.1), which must be set out in the service agreement, be once a month.

f) It is recommended that the commissioning entity require to the service provider that the frequency of the strategic committee meetings (see section IV.4.3.2), which must be set out in the service agreement, be twice a year.

g) It is recommended that the commissioning entity require to the service provider that the frequency of the detection rule status updates (see section IV.2.1.i), which must be set out in the service agreement, be once a week.

h) It is recommended that the commissioning entity choose the strategic and operational indicators which must be set out in the service agreement and which make it possible to measure the service level of the provided service among the indicators suggested by [ETSI_ISG_ISI].

i) It is recommended that the commissioning entity use [ETSI_ISG_ISI] to define the format and content of the security incident tickets.

j) It is recommended that the commissioning entity require the service provider to include in the collection strategy (see requirement IV.2.2.a) the deployment of probes at each of the interconnections of its information system, and, in particular, those interconnections with:

- the Internet;
- third-party information systems (partners, subcontractors, etc.);
- the commissioning entity's other information systems with a lower or more vulnerable security classification or sensitivity level.

k) It is recommended that probes deployed at the interconnections of the commissioning entity's information system be approved by ANSSI at the appropriate level and used in accordance with their technical instructions for use.

l) It is recommended that the commissioning entity:

[13] The catalogue of qualified audit service providers for information system security (PASSI) is published on the ANSSI website.

- synchronise the collection sources hosted on its information system with a single time source;
- develop and implement an event logging policy.

To do this, the commissioning entity may use the ANSSI technical note devoted to the implementation of a logging system [NT_JOURNAL] and use the services of the security incident detection service provider (PDIS) or an approved audit service provider for information system security (PASSI).

m) It is recommended that the commissioning entity use workstations hosted on a dedicated information system that is not interconnected with the information system that is the subject of the service to access the Web portal (see requirement IV.2.3.h) made available by the service provider for managing the security incident tickets.

The purpose of this recommendation is that, in the event that the commissioning entity's information system that is the subject of the service is compromised, the attacker does not have access to security incident tickets enabling it to know whether it has been detected.

n) It is recommended that the commissioning entity put in place a crisis management process in case of the detection of a major security incident within its information system.

o) It is recommended that the commissioning entity require the service provider to integrate into the reporting strategy (see requirement IV.2.3.e) specific reports in the event that major security incidents within its information system are detected.

III. During the provision of the service

a) It is recommended that the commissioning entity regularly transmit to the service provider, throughout the whole of the period that the service is provided, all of the information needed for the service provider to create new detection rules specific to the commissioning entity's needs.

To this end, the commissioning entity may, in particular, submit the results of tests for vulnerabilities and intrusions conducted on its information system.

b) It is recommended that the commissioning entity inform the service provider of any evolution of its information system that could impact the effectiveness of the security incident detection service.

c) It is recommended that the commissioning entity put in place a change management process enabling it to continuously inform the service provider of any changes to its supervised information system (configuration, settings, software versions, etc.).

d) It is recommended that the commissioning entity use an approved security incident response service provider (PRIS)[14] in the event of a suspected or confirmed security incident.

[14] The catalogue of accredited security incident response service providers (PRIS) is published on the ANSSI website.