K21046/02
09-03-2026

Certification scheme

for the Kiwa process certificate concerning the infrastructure and management system for hosted alarm solution providers

creating trust *driving progress*

kiwa

Preface

This International Certification Scheme has been accepted by the Kiwa Board of Experts Security, which includes all relevant parties in the field of security. This Board of Experts also supervises the certification activities and, when necessary, requires the Certification Scheme to be revised. All references to Board of Experts in this Certification Scheme pertain to the Board mentioned above.

This Certification Scheme will be used by Kiwa in conjunction with the Kiwa-Regulations for Certification, which outline the general rules for certification

The publication of this new version of the certification scheme continues to enable the assessment of private hosted alarm solutions as established in the first version. It now also includes the assessment of hosted alarm solutions in public cloud, based on the latest insights. Furthermore the K21046 has been reworked in areas of demarcation, exit strategy, IP routing, change management and shared responsibility.

Kiwa Nederland B.V.
Sir Winston Churchilllaan 273
2288 EA Rijswijk
Postbus 70

Kiwa FSS Certification
Dwarsweg 10
5301 KT Zaltbommel
The Netherlands
Tel. +31 88 998 51 00

Tel. 088 998 44 00
nl.infocertification.fss@kiwa.com
www.kiwa.com

Validation
This certification scheme has been validated by Kiwa on 09-03-2026.

Contents

1 Introduction

1.1 General

This international certification scheme outlines requirements used by Kiwa when processing applications for the issuance and maintenance of process certificates for the infrastructure and management system for Hosted Alarm Solution Providers (HASP).

A Hosted Alarm Solution is designed for hosted alarm processing and handling where the necessary data processing equipment is not confined to a single secure location and is managed by a Hosted Alarm Solution Provider. The HAS comprises various locations, hardware, software and networks, all managed by the Hosted Alarm Solution Provider. This provider is continuously monitoring the functions, security and performance of the Hosted Alarm Solution to arrange Confidentiality, Integrity and Availability. For a high level overview, see figure 1.

The function, performance, reliability, resilience and security requirements of a Hosted Alarm Solution Provider are structured and all components are tested against international standards.

This certification scheme is drafted in the context of EN 50518 and EN 50136 series. Based on these minimum requirements, it enables emerging market developments such as, but not limited to forms of cloud computing, business intelligence and artificial intelligence. These aspects are currently unaddressed in the EN 50518, resulting in ambiguity regarding testability and compliance. This certification scheme can therefore be considered a transitional framework for ensuring clarity in testability and compliance.

The goal of this certification scheme is to support Alarm Receiving Centres (Hosted Alarm Solution Users) in meeting the EN 50518 requirements when using Hosted Alarm Solution technology. It provides a functional certification interface and a shared responsibility model that clearly defines the roles and responsibilities of each party involved.
This ensures that the focus of the external assessment is transparent and well aligned for both the Hosted Alarm Solution Provider and the Hosted Alarm Solution User.

Cloud computing goes hand in hand with issues such as data and digital sovereignty. It is up to the market to define a level for this. This framework addresses the topic and requires a risk-based approach, with the outcome to be included in SLAs and contracts. Kiwa foresees a split in the market on this topic due to European legislation such as NIS, DORA, CRA, CER.

Figure 1. Example of a Hosted Alarm Solution running from two secure locations connected to multiple (MARC) locations

For its certification work, Kiwa adheres to the requirements outlined in EN-ISO/IEC 17065, "Conformity assessment - Requirements for bodies certifying products, processes, and services."

This certification scheme is drafted in accordance with EN-ISO/IEC17067 “Conformity assessment - Fundamentals of product certification and guidelines for product certification schemes”. According to this standard, the scheme is classified as type 6.

The second version of this certification scheme replaces the following:

Certification scheme	Title	Dated
K21046/01	Hosted Alarm Solution (HAS)	2019-02-15

This version of the certification scheme is now ready for immediate use. Existing certificates issued under version one will expire two years after the implementation date of version two.

1.2 Field of application / demarcation

The process certification for a Hosted Alarm Solution Provider covers the management of Hosted Alarm Solution Segments as detailed in 1.2.1. This certification scheme acknowledges two pathways to qualify as a Hosted Alarm Solution Provider:

1. An organization that applies the HAS for its internal organization and/or judicial connected entities.
2. An organization that offers the HAS as a service to third parties and places the HAS on the market for commercial purposes.

Both types of entities can be certified under this scheme for the development, delivery, monitoring, and maintenance processes of a Hosted Alarm Solution provided to a Hosted Alarm Solution User (HAS-U).

The hosting model for the Hosted Alarm Solution Provider (HASP) is categorized into three types: private cloud, public cloud, or hybrid hosting (a combination of public and private cloud).

The technical application scopes are outlined in Table 1. Further details regarding these scopes are provided in clause 4.6.

Where technical application scopes are implemented within the HAS by the Hosted Alarm Solution Provider, they shall be required to meet the provisions of this certification scheme and be explicitly included within the certification scope.

Type HAS Provider	Hosting model	Technical application scope(s)
1 – Internal HAS Provider 2 – Third Party HAS Provider	A - Private B - Public C - Hybrid (combination of both)	- Scope(s) in accordance with EN 50518 Cat I and/or Cat II. - Technical Monitoring Systems (TMS). - Remote Access for Remote Systems (RARS) - Artificial Intelligence (AI) - Business Intelligence (BI)

Table 1 – Demarcation of Hosted Alarm Solution

Based on the demarcation shown in table 1, the requirements of clause 4, 5 and 6 apply to the Hosted Alarm Solution Provider.

1.2.1 Hosted Alarm Solution Segments

In figure 2, a high level drawing is shown, detailing the Hosted Alarm Solution Segments which shall be subject to certification.
Additionally an overview is given in table 2 showing the Hosted Alarm Solution segments with the reference to the clauses in K21046.

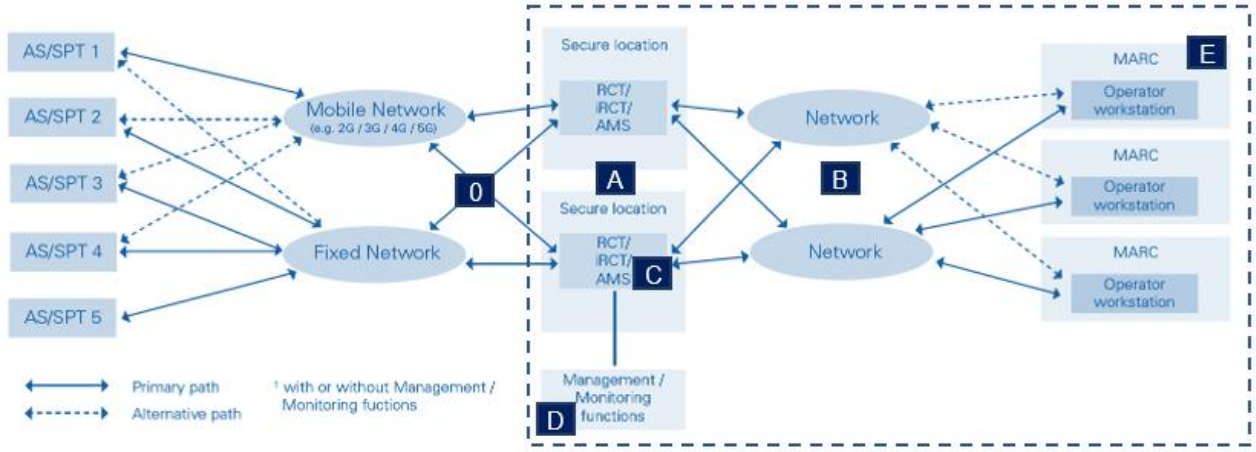

Figure 2 Segments Hosted Alarm Solution

	Hosted alarm solution segment	**Function**	**K21046 reference**
0	IP routing	Connectivity (network) to the SPT's	Clause 6
A	Secure locations	Locations for data processing and storage capacity	Clause 6
B	Critical Alarm Transmission between secure locations and ARC(s)	Connectivity (network) between secure locations and HAS-U (ARC's)	Clause 6
C	Software (RCT, iRCT and AMS)	Data processing equipment for receiving, processing and handling of alarm signals	Clause 6
D	Monitoring activities	Monitoring of all critical Hosted Alarm Solution components in the segments.	Clause 6
E	Service provided to the HAS-U	Enable the Hosted Alarm Solution service at the user	Clause 4 & 5

Table 2: Explanation of the segments of the Hosted Alarm Solution

1.3 Acceptance of test reports supplied by the provider

With regard to the requirements laid down in this certification scheme, the applicant may submit, in the scope of external assessments, reports issued by conformity assessing institutions to prove that the requirements of this certification scheme are being satisfied. It must be demonstrated that the respective analysis/inspection/test and/or evaluation reports have been drawn up by a body that complies with the respective applicable accreditation norm with regard to the subject matter:

- EN-ISO/IEC 17020 for inspection bodies;
- EN-ISO/IEC 17021-1 for certification bodies certifying management systems;
- EN-IEC/IEC 17024 for certification bodies certifying persons;
- EN-ISO/IEC 17025 for laboratories;
- EN-ISO/IEC 17065 for certification bodies certifying products, processes, and services.

Explanation:
An organization will be considered as compliant with these criteria if an accreditation certificate for the respective subject matter can be submitted, issued by the Board of Accreditation (RvA) or another accreditation organization which has been accepted as a member of a multilateral agreement on the

subject of mutual recognition and acceptance of accreditation, which have been drawn up within the EA, IAF and ILAC. If no accreditation certificate can be submitted, the certification organization itself will assess if compliance is given to the accreditation criteria.

1.4 Quality declaration

The quality declaration issued by Kiwa is described as a Kiwa process certificate. Consequently, certification will be granted to the provider responsible for the process that enables the delivery of the Hosted Alarm Solution service. The certificate will clearly specify the demarcation as described in clause 1.2.

A model of the certificate to be issued based on this scheme is included in Annex I for reference.

2 Terminology

2.1 General definitions

In this certification scheme, the following general definitions apply.

2.1.1 Board of experts

the Board of Experts Security.

2.1.2 Certification mark

a protected trademark, the use of which is authorized by Kiwa, may be granted to a provider whose processes are deemed to comply with the applicable requirements upon delivery. Where relevant, quality-related information regarding the product's application may be included. This is communicated through a specially designed label, based on the results outlined in the inspection report issued by Kiwa following the evaluation of the prototype.

2.1.3 Certification scheme

the agreements established by the Board of Experts concerning certification procedures and requirements.

2.1.4 IQC scheme

a description of the quality inspections carried out by the supplier as part of his quality system.

2.1.5 Initial assessment

evaluation carried out to ensure initial conformity with all requirements outlined in the certification scheme.

2.1.6 Surveillance assessment

assessment conducted after the issuance of the certificate to verify that the certified processes continue to comply with the requirements set out in this certification scheme.

Note: The assessment matrix summarizes the scope and frequency of the evaluations Kiwa will perform during both initial and surveillance assessments.

2.1.7 Private Label Certificate

a certificate that applies exclusively to processes also covered under the certificate of a supplier certified by Kiwa. The only distinction is that the products and associated product information of the private label holder are marketed under a brand name owned by the private label holder.

2.1.8 Process certificate

a document issued by Kiwa declaring that a process may, upon delivery, be considered to comply with the process specification as recorded in the process certificate.

2.1.9 Process requirements

requirements that are specified through measurable criteria or defined values, focusing on identifiable characteristics of processes. These requirements include limiting values that must be achieved and can be calculated or measured in an unambiguous manner

2.1.10 Guidance and interpretation document

The Guidance and interpretation document, captures relevant technological and market developments. Its purpose is to clarify the context by introducing new definitions related to specific themes and subjects. This helps individuals and market participants understand the preconditions for determining compliance with applicable requirements.

The document also explains how emerging developments at the level of standards align with market trends and remain consistent with existing legislation and regulations. The Guidance and interpretation document differentiates between 'guidance' and 'interpretation requirements.' This is marked in the document itself and

necessary for compliance to the certification scheme. The document is formally approved by the Board of Experts Security.

2.2 Specific definitions

In this certification scheme, the following specific terms and definitions apply:

2.2.1 Alarm Management system (AMS)

System at a MARC which stores, organizes, controls, manages and allows retrieval of client data and is interfaced to the alarm receiving equipment (RCT) for automatic annunciation of messages for each alarm system. For more information: annex C EN 50518:2019.

[SOURCE: 3.1.4 EN 50518:2019]

2.2.2 Alarm Receiving Centre (ARC)

continuously manned centre where information concerning the status of one or more AS is reported.

2.2.3 Alarm Transmission System (ATS)

Alarm transmission equipment and networks used to transfer information concerned with the state of one or more Alarm Systems at supervised premises to one or more AMSs of one or more MARCs.

Note to entry: An ATS may consist of more than one ATP.

[SOURCE: 4.1.8 EN 50136-1/A1]

2.2.4 Hosted Alarm Solution

A hosted alarm solution as described in this certification scheme.

2.2.5 Hosted Alarm Solution Provider (HASP)

The legal entity and designated provider organization that is responsible for ensuring and managing that all processes, infrastructure, and operations within the defined scope and boundaries of the certification consistently meet the applicable requirements. This responsibility includes:

- Initial compliance: Ensuring that all criteria for certification are met during the initial audit or assessment.
- Ongoing compliance: Continuously maintaining and improving systems and processes to ensure continued adherence to the certification standards.
- Scope management: Clearly defining and managing the scope and demarcation of the certification to ensure relevance and accuracy.
- Accountability: Assigning roles and responsibilities within the organization to oversee compliance, including internal audits, corrective actions, and documentation.

2.2.6 Hosted Alarm Solution User (HAS-U)

The legal entity and designated user organization such as an Alarm Receiving Centre that is responsible for ensuring that all processes, infrastructure, and operations within the defined scope and boundaries of the EN 50518 certification* and / or this certification scheme consistently meet the applicable requirements. This responsibility includes:

- Initial compliance: Ensuring that all criteria for certification are met during the initial audit or assessment.
- Ongoing compliance: Continuously maintaining and improving systems and processes to ensure continued adherence to the certification standards.
- Scope management: Clearly defining and managing the scope and demarcation of the certification to ensure relevance and accuracy.
- Accountability: Assigning roles and responsibilities within the organization to oversee compliance, including internal audits, corrective actions, and documentation.

** EN 50518 or an equivalent assessment and certification.*

2.2.7 Critical Transmission System (CTS)

The transmission system used for critical alarm communication is not end-to-end as defined in EN 50136-1/A1. However, due to its importance for business continuity, this type of alarm transmission is considered critical and requires high uptime.

Note: examples of this critical transmission are:

- *the paths between the RCT-H and RCT-A.*
- *the paths between the Hosted Alarm Solution Provider environment and the Hosted Alarm Solution User environment.*

In these examples, the alarm transmission method may differ from the standard protocols outlined in Annex E of CLC/TS 50136-9. However, any alternative transmission method must comply with the same functional and performance requirements defined in EN 50136-1/A1. Additionally, it must offer Verification of Performance capabilities that are at least equivalent.

Applying the ISO/IEC 62443-3-3 standard is one recognized method to meet these requirements.

2.2.8 Receiver Centre Transceiver (RCT)

An alarm receiver required for receiving and processing incoming alarms.

2.2.9 Secure location

A data processing location that is an ARC category I another location that complies with a published data centre standard with a correct classification**.**

Note 1 to entry: Published data centre standards with minimum classification requirements are listed in clause 6.3.
Note 2 to entry: In other sectors the secure location is mentioned as data center.

2.2.10 Transmission path

The physical connection between the components (external to the housing of the components) used for the transmission of information and/or power.

[SOURCE EN 54-13]

2.2.11 Dual path Alarm Transmission System

The alarm Transmission System consisting of one primary Alarm Transmission Path and one secondary Alarm Transmission Path using diverse technology, having two transmission network interfaces at the Supervised Premise Transceiver, to connect one or more (Wireless Silent) Alarm System of one supervised premises to one or more MARCs.

[SOURCE: 4.1.16 EN 50136-1/A1]

2.2.12 Diverse technology

The technologies used in transmission paths in such a way that a single point of failure, or tampering of a single point, cannot cause both Alarm Transmission Paths of a dual path system to fail simultaneously.

[SOURCE: 4.1.15 EN EN50136-1/A1]

Redundancy is an effective method to prevent a single point of failure from having a critical impact. It enhances the resilience of the infrastructure operated by the Hosted Alarm Solution Provider.
The organization or part of an organization delivering one or more services to a client.

2.2.13 Data sovereignty

The ability to safeguard and have full control over infrastructure, platform, software and data. This results in autonomy of the entity.

Note to entry: This applies in the context of clause 2.2.14

2.2.14 Digital sovereignty

To be in control about the digital environment, ensuring their autonomy in the cyber realm, including data jurisdiction.

2.2.15 Data processing

Any operation or set of operations which is performed on data or on sets of data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

2.2.16 External party

A person or entity that is not under the management responsibility of the Hosted Alarm Solution Provider or Hosted Alarm Solution User.

Note to entry: for example suppliers, installers, cloud providers.

2.2.17 Logical HASP boundary

A logical HASP boundary encompasses all data, systems, users and processes that constitute the data processing of an HASP for the HAS-U and that are under the HASP management policy authority. This boundary excludes third parties that process HASP data under their own policy authority (even if this happens on explicit instructions of the HASP management through a DPA).

Note to entry: The scope of controls do include any interfaces between systems intra-boundary and extra-boundary, i.e. the HASP management is responsible for setting and enforcing policy on any integrations with systems inside the logical HASP boundary, including any remote access facilities.

2.2.18 Private cloud

A dedicated computing environment exclusively used by a single organization. It can be physically located on-site or hosted by a third-party service provider, but all software, infrastructure, platform and services are isolated from other tenants.

2.2.19 Public cloud

A shared computing environment where infrastructure, software, platform or services are provided by third-party cloud providers and used by multiple organizations (tenants).

2.2.20 Service-level agreement (SLA)

A formal agreement between two or more parties to establish a service contract, in which the level of service is formally defined.

2.2.21 Intrusion detection system (IDS)

Information systems used to identify that an intrusion has been attempted, is occurring or has occurred.

[SOURCE: 2.18 ISO 27039]

2.2.22 Virtual Private Network

Restricted-use logical computer network that is constructed from the system resources of a physical network by using encryption and/or by tunnelling links of the virtual network across the real network

[SOURCE: 2.34 ISO 27039]

2.2.23 Key management

Process of handling and controlling cryptographic keys and related material (such as initialization values) during their life cycle in a cryptographic system, including ordering, generating, distributing, storing, loading, escrowing, archiving, auditing, and destroying the keys and related material.

[SOURCE: 3.2.67 IEC 62443-1-1]

2.2.24 Network and Information Security (NIS)

EU-wide legislation on cybersecurity, aimed at establishing a high common level of cybersecurity across all Member States. While it successfully strengthened national capabilities and promoted cooperation, its implementation revealed challenges such as inconsistent application, market fragmentation, and varying levels of preparedness and enforcement among Member States.

2.2.25 Energy Performance of Buildings Directive (EPBD)

A European directive that establishes a unified framework across the EU to enhance the energy performance of buildings. Its objective is to achieve a zero-emission and fully decarbonised building stock by 2050, in alignment with the European Green Deal and climate targets. The directive sets requirements for energy efficiency, renovation of existing buildings, integration of renewable energy sources, and the digitalisation of building systems.

2.2.26 Building Monitoring & Control Systems (BMCS)

Systems designed to monitor and control building operations, such as energy usage, climate control, and system performance. Driven by the Energy Performance of Buildings Directive (EPBD), the demand for BMCS is increasing. This growth underscores the need for secure and reliable Remote Access and Remote Service solutions to support energy efficiency and performance monitoring.

2.2.27 Remote Access & Remote Service (RARS)

Secure and trusted systems that enable remote connectivity to Building Monitoring and Control Systems (BMCS), as defined within the scope of EN 50518 and other relevant technical standards. RARS systems also align with the requirements of the Network and Information Security (NIS) regulation, ensuring cybersecurity and regulatory compliance in remote operations.

2.2.28 Cyber Resilience Act (CRA)

The Cyber Resilience Act (Regulation EU 2024/2847) is a European Union regulation that sets mandatory cybersecurity requirements for products with digital elements. It obliges manufacturers, importers, and distributors to ensure that hardware and software products are secure throughout their entire lifecycle. This includes minimizing vulnerabilities, providing timely security updates, and improving transparency for users.

2.2.29 Critical entities directive (CER)

A European directive aimed at ensuring the continuous delivery of essential services that are vital to society and the economy. It seeks to minimize the impact of both natural and human-made disruptive events by requiring EU Member States to update their national legislation and promptly implement modernized rules that enhance the resilience of critical infrastructure and entities.

2.2.30 Digital Operational Resilience Act (DORA)

An EU regulation designed to ensure that financial entities across the European Union can withstand and recover from ICT-related disruptions such as cyberattacks, system failures, or third-party outages.

2.2.31 Colocation

Colocation (or "colo") in the context of data center infrastructure refers to a facility where businesses can rent space to house servers and other computing hardware. Instead of operating their own data centers, companies place their equipment in a third-party facility that provides the necessary power, cooling, physical security, and network connectivity. This solution is applicable to both private and public cloud environments.

2.2.32 *Data center locations*

Locations of data centers. These are divided on multiple data centers geographically spread. Each location is designed to be isolated from other locations to ensure fault tolerance and disaster recovery.

2.2.33 *Exit Strategy*

A structured approach to disengaging from third-party providers or legacy systems, designed to ensure business continuity, regulatory compliance, and operational resilience. In the context of digital sovereignty (see clause 2.2.16), an effective exit strategy safeguards control over data, infrastructure, and services, enabling organizations to maintain independence and recover operations without external dependency

2.2.34 *Border Gateway Protocol*

A path vector protocol used to exchange routing information between autonomous systems on the internet. Operating over TCP, BGP determines routing decisions based on network paths, policies, and rule sets. It maintains a table of IP prefixes to indicate network reachability, with IP blocks advertised by autonomous systems to signal their ability to route traffic to specific address ranges.

2.2.35 *Control High Privileged Access*

The process of restricting, monitoring, and auditing access to critical systems and data by users or accounts with elevated privileges, in order to minimize security risks, prevent misuse, and ensure compliance with organizational and regulatory requirements.

2.2.36 *Regeling particuliere beveiligingsorganisaties en recherchebureaus (Rbpr)*

The RPBR regulation is legislation that governs the operation and organization of private security companies and detective agencies in the Netherlands. This regulation contains provisions regarding the establishment, operation, and the requirements that security personnel must meet. The purpose of the regulation is to ensure quality and professionalism within the security sector.

3 Procedure for obtaining a certificate

3.1 Initial assessment: general

This clause describes the procedure which the Hosted Alarm Solution Provider (HASP) have to follow to obtain a process certificate from Kiwa. The procedure for surveillance audits in included in clause 8.

The initial investigation will be based on the (process, product and system) requirements as outlined in this certification scheme, including the test methods, and will include the following:

- type testing to determine if the processes meet performance and/or functional requirements;
- infrastructure process assessment;
- assessment of the quality system and the IQC scheme;
- assessment on the presence and functioning of the remaining procedures.

3.2 Initial assessment: specific

The initial assessment will be conducted based on the requirements outlined this certification scheme, including test methods.
Depending on the nature of the system or process to be certified, it will include:

- Establishing the demarcation (configuration) and specifications (categories) of the Hosted Alarm Solution.
- Assessing and evaluating the product quality of relevant components. The candidate Hosted Alarm Solution Provider shall provide an report of accredited laboratory of a self-assessment report with detailed evidence of conformity based on the required standards;
- Assessing and evaluating the secure location(s).
- Assessing and evaluating the network architecture. The candidate Hosted Alarm Solution Provider shall provide a self-assessment report with detailed evidence of conformity based on the required standards;
- Assessing and evaluating the functional, performance and security requirements of the Hosted Alarm Solution. The candidate Hosted Alarm Solution Provider shall provide a self-assessment report with detailed evidence of conformity based on the required standards;
- Assessing and evaluating the availability of the Hosted Alarm Solution. The candidate Hosted Alarm Solution Provider shall provide a self-assessment report with detailed evidence of conformity based on the required standards;
- Assessing and evaluating Hosted Alarm Solution functionalities at the HAS-U;
- Auditing and evaluating the corrective actions taken by the Hosted Alarm Solution Provider in response to communication failures;
- Auditing and evaluating the management system of the Hosted Alarm Solution Provider regarding service delivery;
- Testing the functionality of supporting procedures to ensure they meet the above assessments.

The audit is carried out in two phases:

- Documentation audit: this stage evaluates the potential of the Hosted Alarm Solution to meet the requirements based on documentation and architectural drawings.
- Implementation assessment & audit: this stage assesses the extent to which the system meets the documented requirements through audits and verification of functionalities in the production environment.

3.3 Issuing certificate

After the initial assessment is completed, the results are presented to the decision maker responsible for issuing the certificate. This individual evaluates the results and decides whether the certificate can be granted or if additional data and/or tests are required before issuance.

3.4 Examination of process and/or performance requirements

Kiwa will conduct or commission an examination of the process, and/or performance requirements specified in this certification scheme. Samples required for this examination will be collected by or on behalf of Kiwa.

3.5 Contract review

Optionally, If the Hosted Alarm Solution Provider is not the manufacturer of the process to be certified, Kiwa will assess the agreement between the Hosted Alarm Solution Provider and the producer.
This written agreement, which shall be available to Kiwa, shall include a provision granting accreditation and certification bodies, scheme managers and Kiwa the right to observe certification activities carried out by Kiwa or on its behalf at the producer's site.

4 Organizational requirements for the Hosted Alarm Solution Provider (HASP)

4.1 European standardization framework

The requirements outlined in this certification scheme are used by the certification body to process applications and maintain certification for a "Hosted Alarm Solution". The assessment of the Hosted Alarm Solution is based on the following international standards:

- EN 50136-1; alarm systems - Alarm transmission systems and equipment - Part 1: General requirements for Alarm Transmission Systems (ISO/IEC 60839-5-1);
- EN 50136-3: Alarm systems - Alarm transmission systems and equipment - Part 3: Requirements for Receiving Centre Transceiver (RCT);
- TS 50136-10: Alarm systems - Alarm transmission systems and equipment - Part 10: Requirements for remote access;
- EN 50518 Alarm receiving centres;
- EN 50600 - Data centre facilities and infrastructure and specific Part 2-5 – Security Systems (ISO/IEC 22237-6).

4.2 Governance

The Hosted Alarm Solution Provider- such as the individual(s) responsible for setting objectives, making decisions and executing actions to achieve those objectives- shall ensure the implementation of a robust quality system which emphasizes Confidentiality, Integrity and Availability. Specifically, the provider shall:

- establish the vision, set objectives, provide direction and manage the risks of their organization by defining written strategies which take into consideration the needs and expectations of laws and regulations and all relevant stakeholders (such as clients, employees, shareholders, business partners, insurers, responders, and public authorities);
- implement and maintain adequate measures to fulfil the conditions of this certification scheme;
- implement an ongoing monitoring of the business processes (including internal audits) as well as of the organizational performance;
- establish an ongoing communication with all stakeholders to maintain a high level of awareness in relation to the safety and security oriented services provided.

A quality system aligned with the principles of the harmonized structure is considered suitable to meet these requirements (such as ISO 27001 or comparable). The standards outlined in EN 50518 and EN 50136-1 serve as the foundational basis for the Hosted Alarm Solution Provider’s quality system.

4.3 Management system

The Hosted Alarm Solution Provider shall establish a management system aligned with the scope of this certification scheme. Within this system, the provider shall document and regularly update specific policies and plans addressing the following areas. The Hosted Alarm Solution Provider shall continuously establish conformity with the requirements of this standard through self-assessments.

The Hosted Alarm System Provider shall verify the requirements of this certification scheme based on a reference table detailing the requirements, the position in the management system and the evidence showing conformity.

4.3.1 Management system responsible and product ownership

Top management shall assign the responsibility and authority to ensure that the quality system complies with the requirements of this certification scheme, including the duty to report on its performance to top management.

Additionally, Top management shall assign a product owner responsible for the Hosted Alarm System.

Secure Development Life Cycle (SDLC)
The Hosted Alarm Solution Provider shall establish and maintain a Secure Development Life Cycle (SDLC) framework that ensures security is embedded throughout all phases of software development and maintenance for components in the HAS infrastructure. The SDLC shall at least cover the AMS in accordance with EN 50518 annex C and the RCT in accordance with EN 50136-3.

The Hosted Alarm Solution Provider shall:

- establish and maintain a process which ensures that all changes are formally requested, risk assessed & accepted, deferred or denied. The process covers at least HAS components in line with the requirements of EN 50518 annex C for the AMS and EN 50136-3 for the RCT;
- register any change request in a change register and;
- establish and maintain a process which ensures that changes are properly executed in accordance with the change management process.

4.3.2 Risk and contingency management

The Hosted Alarm Solution Provider shall define and implement a security risk analysis and treatment process that establishes and maintains clear security risk criteria, including:

- criteria for conducting security risk assessments;
- risk acceptance criteria;
- determination of risk levels (based on likelihood and occurrence);
- identification of risk owners;
- selection of appropriate risk treatment options;
- justification for accepted risks.

The risk analysis and treatment plans include motivations for secure locations and/or the location of the Hosted Alarm Solution Provider and the Hosted Alarm Solution User (ARC), and shall consider measures for managing unexpected events. These measures should address prevention, early detection, and response at both the management and technical levels.

The risk assessment and treatment process required by this certification scheme aligns with the principles and general guidelines of ISO 31000. Additionally, ISO 27005 provides specific guidance on managing information security risks.

Aligned with the risk assessment, a Business Continuity Plan shall be developed and maintained. This shall contain realistic fallback plans for technical and non-technical unavailability of cloud infrastructure, platform and software. See clause 7.5.2.

4.3.3 Management of the services portfolio and SLA's

The Hosted Alarm Solution Provider shall for each Hosted Alarm Solution User maintain a service description as part of the contract / SLA detailing all available configurations of the Hosted Alarm Solution in relation to 4.5.

The service description shall:

- Provide clear and unambiguous information to the Hosted Alarm Solution User regarding the scope of the delivered services;
- Clearly define the demarcation of responsibilities between the Hosted Alarm Solution Provider and Hosted Alarm Solution User;
- Specify the performance obligations as outlined in this certification scheme;
- Include how the HASP enables compliance with for clause 6.4.1 of this certification scheme.

The contract/SLA shall cover all relevant clauses in this certification scheme.

In addition, the Hosted Alarm Solution Provider shall maintain an up-to-date service portfolio that includes:

- An overview of services currently available to all Hosted Alarm Solution Users;
- A list of additional services offered;

- Documentation covering the Onboarding , management and offboarding of services Hosted Alarm Solution User.

4.3.4 *Client data management*

The Hosted Alarm Solution Provider shall ensure that all (personal) data supplied by the Hosted Alarm Solution User, including contract and transaction data, is maintained accurately and kept up to date. Furthermore, the provider shall explicitly disclaim liability for third-party actions. These practices must be fully aligned with the requirements of the General Data Protection Regulation (GDPR). The Hosted Alarm Solution Provider shall at least execute and document a self-assessment on this topic.

4.3.5 *Performance criteria management*

The Hosted Alarm Solution Provider shall ensure that all performance criteria are met. A documented procedure shall describe how performance statistics are generated and made available to Hosted Alarm Solution Users demonstrating compliance with the contracted Hosted Alarm Solution services.
All the agreed performance criteria are monitored and reported by the Hosted Alarm Solution Provider.

The Hosted Alarm Solution Provider shall adhere to the performance criteria contractually agreed upon with each Hosted Alarm Solution User, which shall include, at a minimum:

Service availability: 99,9% for all in-scope Hosted Alarm Solution services;
- Response time objective: within 4 hours;
- Recovery time objective: within 8 hours.

There shall be reporting per day, week, month and year. Compliance with these criteria shall be measured over a rolling twelve-month period and reflected upon in a yearly management review. The twelve-month period shall be based on monthly totals.

The weekly, monthly and yearly service availability shall be distributed pro-actively to the Hosted Alarm Solution users.

4.3.6 *Quality of service*

The Hosted Alarm Solution Provider shall implement control measures in accordance with the requirements outlined in EN 50518, to ensure the quality of service meets the performance criteria contractually agreed upon with each Hosted Alarm Solution User.

The control measures shall at least cover:
- Redundancy and availability of HAS components;
- Transmission time in the HAS network;

Quality of service during special conditions (also see 5.8.3)
The Hosted Alarm Solution Provider shall establish and enforce quality of service arrangements under the following circumstances:
- When the provider is no longer able to meet its functional or performance obligations, including access to and retrieval of code and data;
- When the Hosted Alarm Solution User transitions to another Hosted Alarm Solution Provider;
- When the public cloud provider used by the Hosted Alarm Solution Provider is no longer able to meet its functional or performance obligations, including access to and retrieval of code and data;
- When the Hosted Alarm Solution Provider transitions to a different public cloud provider.

4.3.7 *Management of staffing*

All employees in relevant employment of the Hosted Alarm Solution Provider shall be security screened and vetted in accordance with applicable laws, regulations and agreements.
Other than visitors, any person entering the secure locations shall be screened according the security policies of the secure location. Visitors shall be accompanied by an authorized employee at all times while inside the secure location according the security policies of the secure location.

The Hosted Alarm Solution Provider shall adhere to training procedures for all relevant employees covering theoretical and practical skills to comply with the training requirements as laid down by legislation or by the Hosted Alarm Solution Provider.

The Hosted Alarm Solution Provider shall:

- determine the necessary competence of person(s) doing work under its control that affects its information security performance;
- ensure that these persons are competent on the basis of appropriate education, training, or experience;
- where applicable, take actions to acquire the necessary competence, and evaluate the effectiveness of the actions taken; and
- retain appropriate documented information as evidence of competence.

The Hosted Alarm Solution Provider shall design and deliver training for personnel responsible for designing, configuring and maintaining the Hosted Alarm Solution.

The product owner of the Hosted Alarm System shall meet the following requirements:

- Understanding of alarm monitoring technologies and supporting technologies and services (e.g. cloud computing patterns and responsibilities);
- Understanding of standard IT processes (e.g. Information Technology Infrastructure Library);
- Understanding of functional architecture, solution architecture and systems architecture principles and practices;
- Cybersecurity threat exposure and controls to mitigate; e.g. per ISO27001, etc.

4.3.8 Internal audit

The Hosted Alarm Solution Provider shall perform internal audits at least annually to assess its performance to the requirements of this standard.

4.4 Roles and Responsibilities

The Hosted Alarm Solution Provider shall document the roles and responsibilities relevant to the scope of EN 50518 and this certification scheme. This shall be established based on Table 3 that clearly define the respective responsibilities of the Hosted Alarm Solution Provider and the Hosted Alarm Solution User.
In cases were shared responsibility is defined this shall be contractually defined and agreed per SLA between the Hosted Alarm Solution Provider and Hosted Alarm Solution User.

In cases where services are outsourced, the Hosted Alarm Solution Provider shall document the scope of the outsourced activities and shall retain full accountability for the performance and delivery of those services contractually agreed with the Hosted Alarm Solution User.

Requirements ARC facilities (EN 50518)		
Facilities / processes	**Hosted Alarm Solution Provider**	**Hosted Alarm Solution User**
Construction	-	Responsible
Alarm systems	-	Responsible
Electrical power supplies (UPS & Generator)	-	Responsible
Alarm Management System	Shared responsibility	
Telephony	Shared Responsibility	

Requirements Datacentre facilities (Scheme K21046 / EN 50518)		
Facilities / processes	**Hosted Alarm Solution Provider**	**Hosted Alarm Solution User**
Construction (Building)	Responsible - (outsourced to DC)	-
Construction (cage/suite)	Responsible	-
Alarm systems (Building)	Responsible - (outsourced to DC)	-
Alarm systems (cage/suite)	Responsible	-
Electrical power supplies	Responsible - (outsourced to DC)	-
Cooling	Responsible - (outsourced to DC)	-
Fire detection and suppression	Responsible - (outsourced to DC)	-
Access control system	Responsible - (outsourced to DC)	-

Standard Operating Procedures (EN 50518)		
Facilities / processes	**Hosted Alarm Solution Provider**	**Hosted Alarm Solution User**
Creation, modification and cancellation of service or customer accounts	Technical responsibility	Operational responsibility
Message handling	Technical responsibility	Operational responsibility
Communication with response services	Technical responsibility	Operational responsibility
Individual services provided by the ARC	Technical responsibility	Operational responsibility
Alarm verification	Technical responsibility	Operational responsibility
Unexpected increase in alarm signals	Technical responsibility	Operational responsibility
Alarm transmission path failures	Technical responsibility	Operational responsibility
Controls to maintain quality of service	Technical responsibility	Operational responsibility
Installation, maintenance, protection, removal and reuse of assets under the control of the ARC	Equipment within the Hosted Alarm Solution scope is under responsibility of the HASP	Equipment related to operations (generator, ups, safety & security systems) under responsibility or HAS-U
Monitoring and testing of equipment		
Fault procedures and reporting		
Information management		Responsible

Standard Operating Procedures (EN 50518)		
Facilities / processes	**Hosted Alarm Solution Provider**	**Hosted Alarm Solution User**
Data back-up	Technical responsibility	Operational responsibility
Confidentiality and classification of information	-	Responsible
Relationships with essential suppliers	Equipment within the Hosted Alarm Solution scope	Equipment related to operations (generator, UPS, safety & security systems)
Physical access	Responsible (secure locations)	Responsible (ARC)
Remote access	Technical responsibility	Operational responsibility
Operational continuity and emergencies	Technical responsibility	Operational responsibility
Emergency evacuation and re-entry	-	Responsible
Emergency entry	-	Responsible
Key performance indicators	Technical responsibility	Operational responsibility
Performance criteria – message handling	Technical responsibility	Operational responsibility

Table 3 – Roles and responsibilities related to EN 50518 for different perspective

4.5 Setup and demarcation of Hosted Alarm Solution segments

The Hosted Alarm Solution Provider shall document the hosting model provided, including but not limited to private cloud-, public cloud-, and hybrid solutions.

Documentation, as outlined in table 4 shall form part of the Service Level Agreement (SLA). It will define the demarcation of segments and services within the Hosted Alarm Solution.

Additionally, it shall clearly specify the respective shared and separate responsibilities of both the Hosted Alarm Solution Provider and the Hosted Alarm Solution User.

In the context of a risk assessment centred on digital and data sovereignty, the SLA should clearly outline the required safeguards and the associated implications tied to where data is processed and stored.

Hosted Alarm Solution segments	**Hosted Alarm Solution components**	**HAS Provider**	**HAS User**	**Defined in SLA**
Out of scope for HAS	SPT's or other systems such as a VSS enabled to communicate to the Hosted Alarm Solution.		X	
0	IP routing			X
A	Secure location, servers and storage equipment	X		
B	Infrastructure at the Hosted Alarm Solution Provider enabling secure communication from the Hosted Alarm Solution Provider to the Hosted Alarm Solution User	X		

B	Infrastructure at the Hosted Alarm Solution User for secure communication to the Hosted Alarm Solution Provider			X
B	The network infrastructure enabled for Hosted Alarm Solution operations (DC to DC)	X		
C	RCT's enabled to communicate with a SPT's or other systems such as a VSS, iRCT's and AMS	X		
C	iRCT's enabled to communicate with the RCT's and AMS	X		
C	AMS to enable HAS user operations	X		
D	Monitoring equipment	X		
E (Out of scope or arranged in SLA)	Hosted Alarm Solution User network infrastructure for ARC operations		X	X
E (Out of scope or arranged in SLA)	Hosted Alarm Solution User workstation for alarm monitoring including or excluding telephony		X	X
E (Out of scope or arranged in SLA)	Additional services not standard covered such as: • Technical Monitoring Systems (TMS) • Remote Access For Remote Services (RARS) • Business Intelligence (BI) • Artificial Intelligence (AI)			X

Table 4 – Demarcation – Template SLA Hosted Alarm Solution segments and responsibilities

4.6 Requirements for technical application scopes

This clause outlines the technical application scopes. The objective of these additional technical application scopes is to handle processes and data in a secure manner obtaining an acceptable level of confidentiality, integrity and availability.

If the technical application scope for technical monitoring systems is applied, the requirements of EN 50518 series will be included, to for example cooling facilities, in the assessment and specified in the technical approval related to the certification.

Note: this technical application scope should take into account all applicable legislation such as Energy Performance of Buildings Directive (EPBD) and Building Monitoring & Control Systems (BMCS).

If the technical application scope for Remote Access for Remote Service (RARS) is applied, the requirements of EN 50710 and TS 50136-10 will be included in the assessment and specified in the technical approval related to the certification. See also certification scheme K21048 in context with EN50131-1.

If the technical application scope for Business Intelligence (BI) systems is applied, the Hosted Alarm Solution provider shall arrange a analysis which clauses of this certification scheme apply to the infrastructure. However, there is a reduced focus on availability due to its additional nature.

If the technical application scope Artificial Intelligence (AI) systems is applied, the Hosted Alarm Solution provider shall arrange a analysis which clauses of this certification scheme apply to the infrastructure. Clause 4.6.1 details the minimal clauses.

4.7 Use of AI in the Hosted Alarm Solution

Objective: Ensure inherent risk of AI is managed.

4.7.1 AI Register

The Hosted Alarm Solution Provider management shall maintain a register of AI's in use in its Hosted Alarm Solution operation scope. This register shall be kept up to date with minimally a yearly revision.

The register shall contain at least the following information for each AI system used:

General Information

- AI System Name & Description – Brief overview of the system and its purpose;
- Owner & Responsible Department – Who is accountable for the system within the Alarm Receiving Centre organization;
- Vendor/Developer – Whether the AI is developed in-house or sourced from a third party;

AI Use Case & Business Impact

- Purpose & Function – What the AI system is designed to do;
- Decision-Making Role – Whether AI supports, augments, or automates decisions;
- Stakeholders & Affected Groups – Who is impacted by the AI system;

Data & Model Information

- Data Sources – What datasets are used for training and inference;
- Processing of personal data is involved (yes/no);
- Model Type & Algorithms – Machine learning approach (e.g., deep learning, Neuro-Linguistic Programming, decision trees);

Risk Assessment & Mitigation Measures

Inherent risk evaluation, including potential ethical and social impacts;

- Bias & Fairness Evaluation – Steps taken to detect and reduce bias as applicable;
- Explainability & Transparency – Method used for ensuring model interpretability as applicable;

- Security & Robustness – Safeguards against (1) adversarial attacks, (2) data leaks and (3) processing manipulation (e.g. back-doors or fraudulent alarm closing) as applicable;
- Data Privacy Measures – Anonymization, encryption, and consent handling as applicable;
- Human Oversight & Accountability – If and how humans oversee AI decisions;

Monitoring & Lifecycle Management specifications

- Performance Metrics – Accuracy, reliability, and other relevant KPIs;
- Incident & Error Logging – How is a record kept of AI failures or unexpected behaviours;
- Process & responsibilities for AI performance problem management;
- Audit trails of AI behaviour and decisions: data retention and responsibilities;
- Update & Retirement Plan – How and when the AI system will be updated or decommissioned.

4.7.2 Awareness and knowledge

The Hosted Alarm Solution Provider management shall be aware and have access to knowledge on:

- the type of AI used;
- the use case context in which it is deployed;
- the contextual risk exposure of this deployment;
- the compliance requirements;
- the risk management measures, and;
- the operational performance.

Together this awareness and access to knowledge are necessary to take accountability for the AI trained and used in an Hosted Alarm Solution context.

4.7.3 Additional controls

Third-party AI system vendors shall be subject to procedures and controls defined in the process for relationships with essential suppliers' and Risk analysis on third party data processing'.

The Hosted Alarm Solution Provider management shall ensure that AI systems used are designed to resist manipulation and cyberattacks.

It does this by collecting assurance from the vendor when applicable or by performing the required analysis and testing. The Hosted Alarm Solution Provider management shall ensure that AI systems demonstrate reliability and reproducibility in their operation.
Reliability is defined as the system's ability to function correctly under varying conditions, ensuring predictable and consistent performance.
Reproducibility requires that AI systems yield identical results when subjected to the same experimental conditions.
Evidence of reliability and reproducibility shall be documented as part of Alarm verification and Monitoring and testing of equipment.

AI systems shall include fail safe and fall-back mechanisms to ensure they can be disabled without operational disruption of the Hosted Alarm System.

AI systems shall be designed to be understandable and verifiable.

Documentation shall be maintained in compliance with the process for Information Management.
The Hosted Alarm Solution Provider management shall possess adequate knowledge, skills, and understanding to ensure responsible AI deployment. This includes technical, practical, social, and ethical competencies, in alignment with AI regulatory requirements.

5 Operational requirements for the Hosted Alarm Solution Provider (HASP)

5.1 General

The Hosted Alarm Solution Provider shall implement documented procedures and technical solutions for the secure operation of the HAS with a focus per Hosted alarm Solution User.
The focus should be to prevent interference between Hosted Alarm Solution Users if there are more the one Hosted Alarm Solution Users on the same platform and users of the Alarm Management System of the Hosted Alarm Solution User.

Note. If the third party Hosted Alarm Solution Provider enables more than one Hosted Alarm Solution User on the same platform shall the configuration be such that interference from Hosted Alarm Solution User 1 to Hosted Alarm Solution User 2 or another Hosted Alarm Solution User is not possible.

It shall include at least the 7 objectives listed in this clause.

5.2 Objective 1: Control and monitor the Hosted Alarm Solution

Purpose: Keep cyber threats outside of the Hosted Alarm Solution and implement continuous monitoring.

5.2.1 Establish a boundary defence shield

The Hosted Alarm Solution Provider shall implement a boundary defence shield to protect against cyber threats that may attack the Hosted Alarm Solution.

A boundary shield includes as a minimum:

(1) an up-to-date network architecture diagram that documents the Hosted Alarm Solution network and the security controls of the Hosted Alarm Solution boundary;

(2) an effective firewall solution controlling and enforcing a policy on network traffic coming in and out of the Hosted Alarm Solution network environment;

(3) an intrusion detection solution (IDS) that is effective in detecting cyber threats that attempt to cross the boundary shield; and

(4) a solution to protect against distributed denial of service attacks (DDoS).

Note: the boundary defence shield is to be seen in conjunction with the HASP logical boundary.

5.2.2 Investigate communications at the boundary

The Hosted Alarm Solution Provider shall deploy and manage effective solutions to:

(1) secure e-mail systems such that malicious e-mail is kept out of the Hosted Alarm Solution;

(2) allow only legitimate outgoing web traffic;

(3) protect web applications in the Hosted Alarm Solution from incoming web application attacks at application level.

5.2.3 Control Remote Access Connections

The Hosted Alarm Solution Provider shall fulfil following requirements.

Remote Access Connections

The Hosted Alarm Solution Provider shall per Hosted Alarm Solution User shall:

(1) deploy and manage secure solutions and patterns to enable remote access to the logical The Hosted Alarm Solution Provider and Hosted Alarm Solution User boundary for all applicable use;

(2) The remote access procedure shall describe how remote access to and from any system within the Hosted Alarm Solution Provider and Hosted Alarm Solution User and to the receiving data processing equipment (see

5.8) shall be controlled by a log-in / log-out procedure recording time and date, Username of the remote user or remote system involved and actions performed;

(3) Remote access to the Hosted Alarm Solution Provider and Hosted Alarm Solution User shall be constrained on a 'need to know' and 'need to do' basis based on access level/rights in respect to classification of information;

(4) Authentication of remote access shall comply with principle in objective 4.3, Remote access can only be granted and authorized by the Hosted Alarm Solution Provider and Hosted Alarm Solution User. Such access shall be periodically reviewed according to principle in objective 4.2 this review shall as a minimum take place within a 12-month period.

Where the Hosted Alarm Solution Provider and Hosted Alarm Solution User uses web-applications or apps, these web-applications and apps including the servers shall at a minimum be tested at the OWASP-principles including cases where the ARC does not have the management control (see objective 7.1).

Remote Working

All interactive remote access for HASP personnel and third parties shall use a Secure VPN, which requires:

(1) Access only from authorized and compliant devices;

(2) Multi-factor authentication for all users;

(3) Use of IPSec or SSL/TLS-based tunnels;

(4) Access limited to a restricted set of permitted ARC applications/servers;

(5) Dedicated personal accounts;

(6) Granting via formal request and validation;

(7) Time-limited, and subject to recurring review;

(8) Access is permitted only if the accessing device meets required security health conditions (fully patched, host-based protection enabled).

Remote Maintenance

Remote maintenance shall be performed exclusively through authorized screen-sharing solutions that:

(1) Are time-limited;

(2) Are supervised;

(3) Can only be initiated through an time-limited invitation.

External Network Connections

Connections between ARC workstations/networks and external networks shall use Secure VPNs only.

Private and site-to-site VPN connections shall enforce:

(1) Source restrictions (specific remote systems);

(2) Protocol restrictions (only required protocols);

(3)Target restrictions (specific AMS ~~ARC~~ systems);

(4) All site-to-site tunnels must terminate on a central VPN aggregator;

(5) ARC workstations accessing external networks must use secure VPN protocols, have host-based firewalls enabled, and prohibit split tunnelling. These requirements shall be technically enforced, and systems used for outbound remote access shall be network-isolated from the ARC environment.

End-user and installer Web/APP access

Remote access for end-users or installers to access or amend customer data and put a system in test shall use a Secure connection, which requires:

(1) Access only from compliant devices;

(2) Multi-factor authentication for all users;

(3) Use of IPSec or SSL/TLS connection;

(4) Access limited to a restricted set of customer data;

(5) Dedicated personal accounts;

(6) Granting via formal request and validation;

(7) Time-limited, and subject to recurring review;

(8) Access is permitted only if the accessing device meets required security health conditions (fully patched, host-based protection enabled).

5.3 Objective 2: Secure Hosted Alarm Solution infrastructure;

Purpose: Increase internal threat resilience of Hosted Alarm Solution components.

5.3.1 Segment the Hosted Alarm Solution network to contain damage

The Hosted Alarm Solution Provider shall segment the internal Hosted Alarm Solution network into separate network zones to minimize risk concentration per a risk assessment. Zones shall be separated by a network policy controller that limits connections between separate network zones.

Minimally the network zone containing operating processes and the network zones subject to remote access shall be separated from the other data processing areas.

5.3.2 Maintain an Hosted Alarm Solution infrastructure inventory

The Hosted Alarm Solution Provider shall establish and maintain a formalized up-to-date infrastructure asset and application inventory for all assets and applications that are part of the Hosted Alarm Solution.

5.3.3 Manage the configurations and security state of Hosted Alarm Solution Infrastructure

The Hosted Alarm Solution Provider shall implement a solution to:
(1) detect and block malware in its infrastructure;
(2) It will establish and maintain a vulnerability management process that gives visibility to, and minimizes the risk of systems and applications breached through known vulnerabilities;
(3) The Hosted Alarm Solution shall establish, document, maintain, monitor and review configurations, including security configurations, of hardware, software, services and networks;
(4) periodically perform evaluations for the need for penetration tests based on the risk assessment, purple teaming or red teaming exercises to test the threat resilience of Hosted Alarm Solution assets and processes. Attention should be paid on the trustworthiness and quality of the organization that is used;
(5) There shall be documented procedures to describe who may approve and execute the installation, maintenance, disposal and/or reuse of resources, also new HAS users and clients of the HAS user. These shall take into account the specific risks associated with the data and licensed software. The procedure also ensures that unmanaged equipment has appropriate protection.

5.3.4 Enable timely detection and effective response

The Hosted Alarm Solution Provider shall deploy and manage a solution to detect and respond to (potential) intrusions in the Hosted Alarm Solution Provider's networks and/or on systems.

5.4 Objective 3: Secure Hosted Alarm Solution data;

Purpose: Reduce the likelihood of a data breach if other layers of defence would fail and understand the scope of breach in case a data breach would occur.

5.4.1 *Identify sensitive data*

The Hosted Alarm Solution Provider shall:
(1) establish and maintain an up-to-date data inventory and data flow diagram;
(2) Hosted Alarm Solution information assets are classified, labelled and assigned to an owner;
The classification system will explicitly identify any personal data and/or confidential data with respect to the GDPR.

5.4.2 *Protect data (at rest)*

(1) There shall be procedures to describe how all client and system data are backed-up, and to test the availability and reliability of such back-ups. Furthermore, the Hosted Alarm Solution Provider shall deploy and manage;
(2) a solution which protects sensitive data in both production and non-production environments;
(3) It shall also deploy and manage a backup & recovery solution that continuously secures data. This includes encryption of backup data at rest and isolation of at least one recent backup copy from the network;
(4) The backup and recovery solution shall be designed in accordance with Recovery Point Objective (RPO) and Recovery Time Objective (RTO) set by the Hosted Alarm Solution Provider;
(5) The Hosted Alarm Solution Provider shall deploy and manage a solution that manages removable data media in order to avoid data leakage via copying to removeable data.

5.4.3 *Securely exchange Hosted Alarm Solution Data*

The Hosted Alarm Solution Provider shall establish and maintain:
(1) a process which ensures that data exchange instructions and patterns are up-to-date and known;
(2) Contracts with Hosted Alarm Solution Users shall include clauses that specify the mutual responsibilities for sharing Hosted Alarm Solution data;
(3) The Hosted Alarm Solution Provider shall establish and maintain a process which ensures that only secure protocols, encryption and/or tunnels are used when digitally exchanging data with external systems.

Note. Exceptions on secure protocols shall be subject to a cyber security risk assessment.

5.5 Objective 4: Manage Hosted Alarm Solution access

Purpose: Ensure only authorized people and systems get access based on need-to-know and need-to-do principles.

5.5.1 *Manage arrangements and agreements*

The Hosted Alarm Solution Provider shall establish and maintain a process which ensures that data and system access instructions are up-to-date and known by the intended people.

5.5.2 *Manage accounts*

The Hosted Alarm Solution Provider shall manage the access and accounts of internal employees, contingent workers, suppliers and customers;
(1) It shall establish and maintain a process to ensure that accesses are granted after formal validation and removed when no longer needed;
(2) It will also institute a process to ensure that accesses are regularly reviewed and reconciled with the current need-to-know and need-to-do in conjunction with Administrative procedures;
(3) The Hosted Alarm Solution Provider shall deploy and manage a solution to ensure that all accesses are managed and (de)provisioned and contain rules for terminating information access for employees who leave the Hosted Alarm Solution Provider.

This in accordance with the provisions of Clause “Management of Staffing” and “Security screening and vetting”.

5.5.3 *Authenticate in function of the risk*

(1) The Hosted Alarm Solution Provider shall establish and maintain processes which ensure that (1) access to Hosted Alarm Solution assets requires adequate authentication in accordance with an Hosted Alarm Solution Provider password policy;

All (2) interactive accesses to the Hosted Alarm Solution environment from outside the Hosted Alarm Solution boundary shall be subject to multi-factor authentication (MFA).

5.5.4 Control high privileged access

The Hosted Alarm Solution Provider shall establish specific measures to protect the use of high-privilege accounts with additional controls. These shall minimally include:
(1) keeping an up-to-date inventory of high privilege accounts for all Hosted Alarm Solution systems;
(2) a password vault to store the password credentials of such accounts;
(3) periodic rotation of credentials to ensure that high-privilege users are disintermediated from high-privilege passwords not exceeding three months;
(4) The Hosted Alarm Solution Provider shall also enforce separation of duty between password vault control and password usage.

5.6 Objective 5: Control Hosted Alarm Solution changes

Purpose: Avoid that changes have unintended negative results including erosion of the Hosted Alarm Solution Provider's posture.

5.6.1 Control impact when performing changes

The Hosted Alarm Solution Provider shall:

(1) deploy and manage environments where development and tests can be executed without impacting the production environment and allowing to understand the impact of such changes;

(2) leverage these environments such that the risk of a change on the production environment is properly understood and accepted before implementation in the production environment.

5.6.2 Establish a formalized change management process

(1) The Hosted Alarm Solution Provider shall (1) establish and maintain a process which ensures that all changes are formally requested, risk assessed & accepted, deferred or denied;

(2) any change request is registered in a change register and;

(3) establish and maintain a process which ensures that changes are properly executed in accordance with the change management process.

5.7 Objective 6: Ensure incident readiness;

Purpose: Ensure that incidents, when they happen, are dealt with in a controlled manner minimizing the risk that an incident becomes a crisis.

5.7.1 Establish a clear process to handle (cybersecurity) incidents

The Hosted Alarm Solution Provider shall:
(1) deploy and manage a solution which ensures that all systems have the same time as an agreed accurate time source;
(2) Establish and maintain a (cybersecurity) Incident Management process;
(3) make sure that there is a clear and explicit escalation path and criteria to a crisis management process;
(4) ensure that the Data Protection Officer (DPO) is involved in the incident management process when the incident includes a potential breach of personal data; (5) perform a periodic simulation of cybersecurity incidents at least each 12 months, to ensure that processes are tested, known, up-to-date and iteratively improved.

5.7.2 Prepare to recover from severe disasters

The Hosted Alarm Solution Provider shall:
(1) establish and maintain a process and procedure to ensure that a business continuity plan (BCP) exists and is aligned with an (IT) Disaster Recovery Plan (DRP) through setting of recovery point objectives (RPO) and recovery

time objectives (RTO) in line with and include sufficient detail to describe how monitoring services will be restored;
(2) The Hosted Alarm Solution Provider shall establish and maintain a Disaster recovery Plan for all Hosted Alarm Solution applications;
(3) It shall perform periodic disaster recovery testing of data, systems and applications not exceeding 12 months.

The RPO and RTO shall be in line with clause 4.3.5.

5.8 Objective 7: Control Hosted Alarm Solution data processing by external parties

Purpose: Reduce the likelihood that external party data processing becomes a vector of a data breach/violation, data loss or unavailability of the Hosted Alarm Solution.

5.8.1 Control contracting, responsibility and requirements for data processing

Hosted Alarm Solution related data processing can be organized under the direct policy authority of the Hosted Alarm Solution Provider management. In that case the Hosted Alarm Solution Provider management is responsible for the organization and performance of the required controls for the software, infrastructure and platform layers as specified in table 5. In this case the data processing takes place within the logical Hosted Alarm Solution boundary.

The data processing can also be contracted partly (parts of the software, infrastructure and/or platform layers) to an external party that has its own policy authority. In this case parts of the data processing takes place outside the logical Hosted Alarm Solution Provider boundary and the external party has an outcome obligation.

Another option is contracting for knowledge to assist the Hosted Alarm Solution Provider management.
This only covers an effort obligation in accordance with 4.3.7. The Hosted Alarm Solution Provider shall keep a register of data processing activities by the Hosted Alarm Solution and by external parties.

Controls and requirements that shall always stay under the responsibility of the Hosted Alarm Solution Provider Management and that cannot be delegated to an external party are:

- Identity & Access Management for accesses that allow performing Hosted Alarm Solution Provider activities or accessing HAS data;
- Encryption mechanisms for shielding external parties from HAS data at rest or in transit based on industry best practices. The encryption mechanisms shall be under the Hosted Alarm Solution Provider responsibility and should be logically separated from the cloud provider.

5.8.2 General principles for data processing

1.Where an external party undertakes data processing or provides elements of the data processing environment, the Hosted Alarm Solution Provider management shall impose equivalence of security requirements and controls between the Hosted Alarm Solution Provider policy domain and the external party's policy domain. The equivalence of controls shall be in line with EN 50518.

2. Where the Hosted Alarm Solution Provider management delegates Hosted Alarm Solution related data processing - in whole or part - to an external party, this shall be governed by a contract.
This contract shall establish responsibility for the implementation and maintenance of security requirements and controls, and explicitly identify the security requirements and controls that are managed:

- By the HAS Provider management;
- By the external party;
- Between the HAS Provider management and the external party.

The contract shall specify the assurance mechanisms required by the Hosted Alarm Solution Provider management to demonstrate compliance with the first paragraph of this subclause.

The external party provider is responsible for collecting adequate assurance from its own suppliers and providing it to the Hosted Alarm Solution Provider management. Typical assurance mechanisms include control

performance reporting, periodic service management meetings and relevant independent certification of control performance.

The Hosted Alarm Solution Provider management shall ensure that the contract with the external party cover service levels, handling of security incidents, back-up and recovery, an exit strategy with a plan/procedure in conjunction with this certification scheme and if applicable, GDPR compliance requirements such as a Data Protection Agreement (DPA) and governance with respect to subcontractors.

3.Where delegated processing of Hosted Alarm Solution data is being considered or is in place, a documented risk assessment shall be undertaken to identify and determine the management of risks that arise from the delegation of Hosted Alarm Solution data processing to an external party. This risk assessment shall be reviewed at least annually.

The risk assessment shall identify treatment (accept, avoid, mitigate, transfer) of all the identified risks and actions relevant to that treatment; as a minimum the risk events shall include:

- Data breach at the external party;
- Data and digital sovereignty;
- Unavailability of service;
- External party reliability (screening); and
- Continuity.

The contract (including any addenda) shall reflect and be consistent with the actions identified in the risk assessment.

	Who is responsible for implementation and maintenance of security requirements and controls	**How to arrange by the HASP management What may be provided by subcontract**
HAS OPERATIONS		
Client data	HASP	Expertise
SOFTWARE		
AMS / Database	HASP or external party	Expertise/Services
AMS User Management (IAM)	HASP	Expertise
AMS Configuration Management	HASP or external party	Expertise/Services
ATS/RCT	HASP or external party	Expertise/Services
INFRASTRUCTURE		
IT Security	HASP or external party	Expertise/Services
Encryption / Key management	HASP	Expertise
Network Components	HASP or external party	Expertise/Services
Network Components on site /routers/switches/firewalls	HASP or external party	Expertise/Services
Network Configuration Management	HASP or external party	Expertise/Services
PLATFORM		
OS user management (IAM)	HASP	Expertise
OS / Compute / Storage	HASP or external party	Expertise/Services

Hardware / Virtualization	HASP or external party	Expertise/Services
NOTE The HASP management remains accountable also where the responsibility is delegated to an external party		

Table 5 – contract, responsibility and controls for data processing

5.8.3 Exit strategy for data processing

There shall be a documented exit strategy for the HAS provider in context of the HAS user. The HAS provider shall include external parties in this documentation when this is applicable.

The process shall be effective within the agree SLA timeframe. The process shall be periodically tested resulting in a report with functionalities and performances in line with the risk assessment.

Note: Providing a dump of the database every 24 hours to the HASP can be seen as a part of the solution for digital and data sovereignty taking into account the key management system.

6 Technical Requirements for the Hosted Alarm Solution Provider (HASP)

6.1 Infrastructure

The Hosted Alam Solution Provider shall develop and adequately maintain an ICT infrastructure drawing detailing redundancy (N+1) throughout the whole ICT infrastructure in order to achieve the 99,9% availability.

The infrastructure shall be capable of enabling the necessary processing in accordance with EN 50518 and transmission times in accordance with EN 50136-1.

6.1.1 IP routing (Segment 0)

The Hosted Alarm Solution Provider or Hosted Alarm Solution User shall manage the public IP addresses.

The hosting location of the IP-blocks or other technical comparable solution shall be at least at the level of ISO/IEC 27001.

6.2 Secure locations (Segment A)

Data processing in a remote location from the Hosted Alarm Solution shall take place in secure location which is either another category I ARC or a location that complies with the requirements in 6.2.1 or 6.2.2.

The following requirements shall be implemented for each data processing in a secure location:

- Where data processing involves external parties, it shall comply with clause 5.8.

6.2.1 Private Cloud

This clause outlines the requirements that the system must meet when hosted in private cloud.

Geo redundancy & duplication of data	Uptime criteria & evidence statistics	Required data centre certification	Availability & security data centre controls
A minimum of two physically separated locations with a minimum distance of at least 10 km and based on the threat on regional disturbances; Both shall be located within the EU GDPR region; Data and digital sovereignty shall be in scope of the risk assessment of the HASP.	99,9% over the services required by the HASP	A data centre (colocation) designed and maintained according to the following classifications: EN50600 availability class 3 or comparable. in context with EN50518. Or in a category I (ARC) secure shell according to EN 50518 (in this case, the availability and security requirements in the right column do not apply).	The following controls shall be either arranged by the hosting / cloud service provider and/or the HASP: **Availability** - Power (N+1); - Connectivity (N+1); - Cooling (N+1); - Fire compartment (30 minutes); - Automatic Fire Protection System (FPS) for the DC. **Security** - The data processing and storage equipment dedicated to the HASP shall be located within a private cage or suite; - Security zones / protection classes (minimum of 3) including an access control system (ACS) for both the data centre and the private cage. - Intrusion and hold-up alarm system (I&HAS) for the private cage; - Dual Path 4 Alarm Transmission system (ATS) for the private cage. - Video Surveillance System (VSS) for both the data centre and the private cage. - All systems and installations shall be maintained annually in accordance with applicable (local) standards; - Identification (and screening of staff, where needed) by the HASP of those people who enter the cage/suite at the DC.

Table 6 high level requirements hosted alarm solution in private cloud.

6.2.2 Public cloud

This clause outlines the requirements that the system must meet when hosted in public cloud.

Geo redundancy & duplication of data	Uptime criteria & evidence statistics	Required data centre certification	Availability & security data centre controls
3 Data Center Locations All within the EU GDPR region; Data and digital sovereignty shall be in scope of the risk assessment of the HASP.	99,9% over the services required by the HASP. The uptime requirement for the HAS service remains 99,9%.	The cloud service provider shall provide evidence of compliance based on valid certification to: - ISO27001 - ISO27017 - SOC2 (type II) - C5 standard Note: the C5 certificate and report is acceptable evidence of compliance. The report contains evidence in respect of EN 50600 standards.	The following controls are at least included in scope of certification / assurance: - Access control for building and terrain; - I&HAS and ATS; - VSS; - Automatic Fire Protection; System (FPS); - Screening procedure for DC staff.

Table 7 - high level requirements for hosted alarm solution in public cloud

6.2.3 *Hybrid cloud*

Where combinations of private and public cloud are used, the requirements for both secure locations shall be met. For private cloud table 5 and for public cloud table 6. The interoperability shall be managed by the Hosted Alarm Solution Provider.

Note: an example could be where the AMS is hosted in private cloud and the receivers are hosted in public cloud.

In case of fall back scenario's, the set-up shall be detailed in the business continuity plan. For example, in this scenario only one server room in an certified ARC category I is possible.

6.3 Network (Segment B)

The network between the Hosted Alarm Solution Provider secure locations and the Hosted Alarm Solution Users, seen as Critical Transmission System (CTS) shall comply with EN 50136-1/A1, applying the DP4 requirement of 99.9% availability and a minimum 256-bit encrypted tunnel with end-to-end encryption from device to device (e.g. VPNs).

Where other technologies for communication are used, such as RDS, these shall be mapped with the requirements of EN 50136-1/A1.

Where video transmission is applicable, the requirements of this clause apply. However, the protocols and components used shall be based on the agreed requirements in the SLA and shall at least be at a comparable level of EN 50136-1.

Note: Diverse technology should be taken into account in the network as much as possible

6.4 Software (Segment C)

6.4.1 *AMS*

An Alarm Management System (AMS) shall be a software-based system for receiving, generating, storing, processing, forwarding and presenting alarm-related messages and associated data.
The AMS shall support reception and processing of both automatically generated and manually triggered messages.
The intended use of the AMS shall be declared and documented and shall determine applicable additional requirements.

System architecture
The AMS shall operate as software on one or more computers with persistent physical data storage.
The AMS may consist of multiple logical or physical modules, provided that all required functions are fulfilled.
Where additional functions are provided, these additional functions shall not interfere with the reception, processing, performance and presentation of alarms and messages.

Interfaces and interconnections
The AMS shall provide at least one message input interface.
As a minimum the AMS shall support the following interfaces and interconnections:

- interconnection with RCT's (RCT-A and/or RCT-H) compliant with EN 50136-3;
- interconnection with other AMSs with equivalent or higher security and performance;
- communication with external devices and information systems, where applicable.

All supported interfaces and interconnections shall be monitored, documented and tested.

Message handling
All received messages shall be securely stored prior to processing.
Alarm and fault messages that require operator action shall be presented to the operator within defined time limits and shall trigger a visual and/or audible indication.
The AMS shall include a message queue with a calculated and documented minimum capacity, prioritization rules and overload indication.

The AMS provides a facility to set input priorities, the messages should be retrieved according to the priority levels. The method of defining the input priorities should be given by the manufacturer in its documentation (for example type of alarms, grade, etc.). Where a number of messages of equal priority are in the queue they should be retrieved in the order of their arrival.
Expected messages, received by the AMS within the agreed pre-planned time periods, need not be presented, provided that following acknowledgement, processing is carried out automatically by the AMS. If expected messages are not received by the AMS and acknowledged within the pre-planned time periods, a message should be generated by the AMS and processed as specified in
The AMS should allow presentation of expected messages on demand.
Incoming messages shall not be acknowledged if the AMS is unable to correctly store and/or process them.

User interface and access control
The AMS shall not be operable without prior successful authentication by an operator.
The AMS shall implement role-based access control with multiple access levels.
All logon, logoff and configuration and software changes shall be logged. Logs shall be kept for a minimum of 3 years.
The AMS shall display all information required for message processing, including object identity, message type, timestamps and priority.

Master data
The AMS shall provide functions for managing master data by authorized users.
Master data changes shall be logged, and reconstruction over a minimum of three years shall be possible.
Manual data entry shall be subject to plausibility checks.

Fault monitoring
The AMS shall continuously monitor the availability and performance of both hardware and software components.
Detected faults shall be indicated and logged within defined and documented time limits.

Logging, time and traceability
The AMS shall maintain persistent logs for all received events, master data and system interactions.
All timestamps shall use UTC with at least one-second resolution and an accuracy within maximum 10 seconds per annum. Continuous automatic time synchronization of all AMS (sub)systems with one or more time servers is mandatory.

Log data shall be protected against loss, erasure and unauthorised modification.
Access to log data shall be restricted to authorised users.

The AMS shall comply with requirements in this clause 6.4.1.

It may show also show compliance based on EN 50518 clause 8, annex C or VDS 3534.
This enabling the processes according to EN 50136-1/A1 (IEC 60839-5-1).
The candidate Hosted Alarm Solution Provider shall provide a self-assessment report with detailed evidence of conformity based on the required standard.

Note. The assessment based on VDS 3534 directing to VDS 2465 and VDS 3895 can also be handled based on another industrial protocol / solution. Where the requirements direct to an inspection by VDS can this be also Kiwa.

6.4.2 RCT

The RCT shall comply with requirements based on EN 50136-3. The Hosted Alarm Solution Provider shall provide an report of accredited laboratory or a self-assessment report with detailed evidence of conformity based on the required standards.

Where video transmission is applicable, the requirements of this clause apply. However, the protocols and components used shall be based on the agreed requirements in the SLA and shall at least be at a comparable level of EN 50136-1.

6.5 Monitoring (Segment D)

The segments, networks and components shall be monitored continuously in accordance with EN 50136-1/A1 under the responsibility of the HASP. This includes KPI's for performance and the security of the infrastructure.

The monitoring shall at least contain:

- Uptime;
- Latency (between Hosted Alarm Solution Provider and Hosted Alarm User) ;
- Security.

7 Marking

7.1 General

The systems, processes and services shall be marked with a declaration of conformity according this certification scheme and applicable standards. The declaration shall contain at least the following information:

- name or logo of the supplier or manufacturer;
- data or code indicating the date of delivery or maintenance;
- type indication;
- certification marking according this scheme.

Indications and markings shall at least fulfil the requirements in the relevant standard.

7.2 Certification mark

After concluding a Kiwa certification agreement, the certified process shall be indelible marked with the certification mark as is detailed in this scheme.

8 Summary of tests and inspections

8.1 General

This clause summarizes assessments to be conducted for certification:

- **initial investigation:** assessment to ensure all requirements in the certification scheme are met;
- **assessment after granting of certificate:** assessment conducted after the certificate is granted to verify that certified products continue to meet the requirements in the certification scheme.
- **Assessment of the quality system of the supplier:** monitoring compliance of the IQC scheme and procedures.

8.2 Assessment matrix

Description of requirements	**Clause no. scheme**	**Within the scope of:**	
		Initial assessments by Kiwa	**Surveillance assessments by Kiwa after granting the certificate** a,b)
Management system	4	X	X
HASP operating procedures	5	X	X
Technical Requirements	6	X	X
Marking	7	X	X

Table 8 – assessment matrix

- In case the product or process changes, it must be determined whether the performance requirements are still met.
- All characteristics that can be determined within the visiting time are determined by the assessor or by the provider in the presence of the assessor. In case this is not possible, an agreement will be made between the certification body and the provider about how the assessment will take place. The frequency of the assessment visit is defined on a minimal of once per year.

8.3 Inspection of the quality system of the Hosted Alarm Solution Provider

The quality system with cyber security controls of the supplier will be checked by Kiwa on the basis of the IQC scheme. The inspection contains at least those aspects mentioned in the Kiwa Regulations for Certification.

8.4 Additional guidance by the Board of Experts

The board of experts may develop additional guidance and interpretations to define the context of the requirements and to clarify their objectives and meanings.

9 Requirements for the Certification Body

9.1 General

Beside the requirements included in these certification scheme, the general rules for certification as included in the Kiwa Regulations for Product Certification also apply.
These rules are in particular:

- the general rules for conducting the pre-certification tests, in particular:
  - the way suppliers are to be informed about how an application is being handled;
  - how the assessment is conducted;
  - the decision to be taken as a result of the pre-certification assessments.
- the general rules for conducting inspections and the aspects to be audited,
- the measures to be taken by Kiwa in case of non-conformities,
- the measures taken by Kiwa in case of improper use of Certificates, Certification Marks, Pictograms and Logos,
- terms for termination of the certificate,
- the possibility to lodge an appeal against decisions of measures taken by Kiwa.

9.2 Certification staff

The staff involved in the certification may be sub-divided into:

- Certification assessor (**CAS**): in charge of carrying out the pre-certification tests and assessing the inspectors' reports;
- Site assessor (**SAS**): in charge of carrying out external inspections at the supplier's works;
- Product manager (**PM**): Define and maintain the scheme plan, that addresses requirements related to the assessment scheme that (s)he is assigned to**;**
- Reviewer: (**RV**) Conduct the review prior to making a certification decision;
- Decision maker (**DM**): in charge of taking decisions in connection with the pre-certification tests carried out, continuing the certification in connection with the inspections carried out and taking decisions on the need to take corrective actions.

9.3 Qualification requirements

The qualification requirements consist of:

- qualification requirements for personnel of a certification body which satisfies the requirements in table 9, performing certification activities;
- qualification requirements for personnel of a certification body performing certification activities set by the Board of Experts for the subject matter of this certification scheme;
- Education and experience of the concerning certification personnel shall be recorded demonstrably.

Basic requirements	**Evaluation criteria**
Knowledge of company processes Requirements for conducting professional audits on products, processes, services, installations, design and management systems.	*Relevant experience: in the field* **SAS, CAS, PM** : 1 year **DM**: 5 years inclusive 1 year with respect to certification Relevant technical knowledge and experience on the level of: **SAS, CAS, PM** : High school **DM** : Bachelor
Competence for execution of site assessments. Adequate communication skills (e.g. reports, presentation skills and interviewing technique).	**SAS, CAS**: Kiwa Audit training or similar and 3 site assessments including 1 autonomic under review.
Execution of initial examination	**SAS, CAS**: 3 initial audits under review.

Basic requirements	Evaluation criteria
Conducting review	**RV**: conducting 3 reviews.

Technical competences	Evaluation Criteria
Education	**General**: Education in one of the following technical areas: • Electronical Engineering; • Security Engineering; • Safety Engineering.
Testing skills	**General:** • A laboratory training (general and scheme specific) including measuring techniques and performing tests under supervision or Internal training witness testing ; • Conducting tests (per scheme).
Experience - specific	**CAS & PM** • 1 complete applications (excluding the initial assessment of the site) under the direction of the **PM / CAS** • 1 complete application self-reliant (to be evaluated by **PM / CAS** • 1 initial assessments of the site under the direction of the **PM / CAS** • 1 initial assessment of the site self-reliant (witnessed by **PM / CAS**) **SAS** • 2 inspection visits together with a qualified **SAS** • 1 inspection visits conducted self-reliant (witnessed by **PM / CAS**)
Specific knowledge	**CAS & SAS & PM** • EN50136-1, 2 and 3 • EN50600-2-5 • EN50518 • ISO27001 • ISO22301 • Cloud architecture • Cloud Security • IT General controls • SDLC • ITIL
Skills in performing witnessing	**PM & SAS & CAS** Internal training and qualification

Table 9 qualifications

Legend:

- Certification assessor (**CAS**)
- Decision maker (**DM**)
- Product manager (**PM**)
- Reviewer (**RV**)
- Site assessor (**SAS**)

9.3.1 Qualification

The qualification of the Certification staff shall be demonstrated by means of assessing the education and experience to the above-mentioned requirements. In case staff is to be qualified on the basis of deflecting criteria, written records shall be kept.

The authority to qualify staff rests with the:

- **Unit manager**: qualification of **CAS, SAS, RV** and **PM**;
- Management of the certification body: qualification of **DM**.

9.4 Report initial investigation

The certification body records the results of the initial investigation in a report.
This report shall comply with the following requirements:

- completeness: the report provides a verdict about all requirements included in the certification scheme;
- traceability: the findings on which the verdicts have been based shall be recorded and traceable;
- basis for decision: the **DM** shall be able to base his decision on the findings included in the report.

9.5 Decision for granting the certificate

The decision regarding the granting of a process certificate or the imposition of measures related to the product certificate shall be based on the findings documented in the file.
The results of an admission investigation and a periodic assessment (in the event of a critical deficiency) shall be reviewed by a reviewer.
Based on the completed review, the decision-maker determines whether:
• The process certificate can be granted,
• Sanctions are to be imposed,
• The process certificate shall be suspended or withdrawn.
The reviewer and the decision-maker must not have been involved in the creation of the findings on which the decision is based. The decision must be recorded in a traceable manner

9.6 Layout of quality declaration

The product certificate shall be in accordance with the model included in the Annex.

9.7 Nature and frequency of third-party audits

The certification body shall conduct regular surveillance assessments / audits at to ensure compliance with their obligations. The frequency of these audits is determined by the Board of Experts.

Upon the implementation of this scheme, the frequency of on-site assessment / audits is set at one assessment / audit per year for, where the IQC scheme is an integral part of the quality management system.

The audit programme is such that all requirements are assessed during the initial and surveillance assessment / audits.

9.8 Non conformities

When the certification requirements are not met, measures are taken by Kiwa in accordance with the sanctions policy as written in the Kiwa Regulation for Certification.
The Sanctions Policy is available through the “News and Publications” page on the Kiwa website.

9.9 Report to the Board of Experts

The certification body shall provide an annual report detailing the certification activities performed. This report shall include the following aspects:

- Changes in the number of issued certificates (granted/withdrawn);
- Number of audits conducted relative to the required minimum;
- Results of the assessments;
- Required measures for addressing established non-conformities;

- Complaints received about certified products.

9.10 Interpretation of requirements

The Board of Experts may record the interpretation of requirements of this certification scheme in one separate guidance and interpretation document.

9.11 Specific rules set by the Board of Experts

The Board of Experts has defined the following specific rules, which shall be adhered to by the certification body:
Compliance audits are carried out annually by a body accredited for EN 50518 and ISO27001 based on EN-ISO/IEC17065 and -17021-1 in accordance with EA MLA (European Cooperation for Accreditation).

10 Titles of standards

10.1 Regulations

NL-Rpbr	Regeling particuliere beveiligingsorganisaties & recherchebureaus. *Note. Applicable for the Netherlands*
GDPR	REGULATION (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation GDPR). *Note. Applicable for the EU.*
EDPB	EDPB Guidelines on processing of personal data through video devices adopted on 10 July 2019, if applicable.
NIS	DIRECTIVE (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union. (NIS Directive) with update to NIS2, if applicable.

10.2 Standards / normative documents

Number	Title	Version*
EN50136-1 also IEC 60839-5-1	Alarm systems - Alarm transmission systems and equipment - Part 1: General requirements for alarm transmission systems	2012 A1/2018 2013
EN 50136-2	Alarm systems - Alarm transmission systems and equipment - Part 2: Requirements for Supervised Premises Transceiver (SPT)	2013
EN 50136-3	Alarm systems - Alarm transmission systems and equipment - Part 3: Requirements for Receiving Centre Transceiver (RCT)	2013
TS 50136-10	Alarm systems - Alarm transmission systems and equipment - Part 10: Requirements for remote access	2022
EN 50518	Monitoring and alarm receiving centre's	2019
EN 50600-1 also IEC 22237-1	Information technology - Data centre facilities and infrastructure - Part 1: General	2012
EN 50710	Requirements for the provision of secure remote services for fire safety systems and security systems	2021
EN ISO/IEC 27001	Information Security Management System	2022
ISO/IEC 62443-3-3	Industrial communication networks - Network and system security - Part 3-3: System security requirements and security levels	2019
VDS 3534	Guidelines for Computer-Based Information Systems - Alarm Management Systems - Requirements	2023
K21048	Remote Access for Remote Services (RARS) Certification Scheme	2025

*) When no date of issue has been indicated, the latest version of the document is applicable.

I Model certificate (example)

Certificate

Process Certificate
K-XXXXXXX-X

kiwa

Issued	Fill in date
Valid until	Indefinite
Page	1 of 2

Hosted Alarm Solution

Statement by Kiwa
Kiwa states with this process certificate, issued in accordance with the Kiwa Regulations for Certification, that there is legitimate confidence that the service provided by

Name of business

meets the requirements of the scheme K21046 "Hosted Alarm Solution - for the infrastructure and processes for hosted alarm handling" dated 01-04-2026 for the scopes defined on page 2 of this certificate.

Kiwa Nederland B.V. gives the certification trademark in license to Bedrijf for the service performed under certificate.

Signature

Wim van Loon
Managing Director Nederland

Publication of this certificate is allowed. Consult www.kiwa.com in order to ensure that this certificate is still valid. This certificate remains the property of Kiwa.

Version

Kiwa Nederland B.V.
Sir Winston Churchilllaan 273
Postbus 70, 2288 AB Rijswijk
Tel. +31 (0)88 998 44 00
www.kiwa.com

Executed by:
Kiwa FSS Certification
NL.infocertification.fss@kiwa.com

Hosted Alarm Solution Provider
Bedrijf
Adres
website

Extra information customer
onderregels vrij invulbaar maken

Certificate
K-XXXXXXX-X

Hosted Alarm Solution

Scopes and configurations
1. An organization that applies the Hosted Alarm Solution for its internal organization and/or judicial connected entities.
2. An organization that offers the Hosting Alarm Solution as a service to third parties and places the HAS on the market for commercial purposes.

Hosting configuration
A. Private
B. Public
C. Hybrid (combination of both)

Technical application scope(s)
- Scope(s) in accordance with EN 50518 Cat I and/or Cat II:
  - Intrusion & Holdup Alarm Systems;
  - Access control systems;
  - Video Surveillance Systems in security applications that require an emergency response (for example loss prevention);
  - People monitoring, lone workers and object tracking systems for security applications;
  - Alarm messages handled by category II ARCs;
  - Fire alarm systems;
  - Fixed firefighting systems;
  - Social alarm systems;
  - Audio/video door entry systems;
  - Video Surveillance Systems in non-security applications (for example traffic flow);
  - People monitoring, lone workers and object tracking systems for non-security applications;
  - Lifts emergency systems;
- Technical Monitoring Systems (TMS);
- Remote Access for Remote Systems (RARS);
- Artificial Intelligence (AI);
- Business Intelligence (BI).

Technical specification scope
The processes and infrastructure are intended to be used for the handling of alarms in a hosted alarm solution.
An Hosting Alarm Solution platform is a solution for the processing of alarms, where the processing and/or handling equipment is not only (or not) in the alarm receiving centre, but in data centres or distributed over multiple alarm reception centre locations. With an Hosting Alarm Solution platform, the customer, being the alarm receiving centre, is supported with respect to the technical set-up and continuity of alarm reception, processing and handling. By placing the required infrastructure and equipment in data centres or EN 50518-certified locations and spreading it over multiple locations (redundancy), there is a much higher degree of availability. The customer connects to the servers via a secure session, which enables alarm handling in the alarm management software via a client.

An Hosting Alarm Solution platform consists of locations, hardware, software and network(s). All of this is under the control of a Monitoring- or/and Alarm Receiving Centre that performs the same function. There are always at least two locations so that continuity of service can be guaranteed. If one of the locations should drop off due to unforeseen circumstances, the service will not be interrupted, due to the availability of the other location(s). This concerns a total solution for infrastructure, equipment and alarm management system.

Certificate
K-XXXXXXX-X

Hosted Alarm Solution

All the above components are tested against European standards. The delivery of an Hosting Alarm Solution platform requires:
A. A location or locations that meet the criteria set in EN 50518 and/or EN 50600;
B. An alarm receiver/processor (RCT=B1 and iRCT=B2) that functionally meets the requirements set in EN 50136-3 and is compatible with a defined alarm transmitter (Supervised Premises Transceiver (SPT));
C. A network between the customer and the RCT as part of EN 50136-1;
D. A management system, as described in Requirements for the management system, which is focused on the performance of the HAH platform and produces periodic reports, which are sent directly to the end-user if necessary. In addition, the Plan-Do-Check-Act (PDCA) cycle is used, with which corrective and preventive measures are taken if the HAH platform does not meet the performance requirements;
E. Alarm management software required for the handling of alarms within an EN50518-approved alarm centre;
F. The monitoring or alarm receiving centre that collects the data and handles alarms according to requirements and thus meets the criteria set in EN 50518.

Marking for this process

kiwa
CERTIFIED
K21046
HOSTED ALARM
SOLUTION

RECOMMENDATIONS FOR CUSTOMERS

Check at the time of delivery whether:
- the supplier has delivered in accordance with the agreement;
- the mark and the marking method are correct;
- the service show no defects.

If you should reject a product / service on the basis of the above, please contact:
- Bedrijf

and, if necessary,
- Kiwa Nederland B.V.

Consult the supplier's processing guidelines for the proper storage and transport methods.

II Model IQ-scheme (example)

Inspection subjects	Inspection aspects	Inspection method	Inspection frequency	Inspection registration
Infrastructure: - Layout; - Functions - Performance - Security	According scheme	According scheme Design Testing configuration Commissioning Verification Handover Maintenance	Setup Ongoing	According scheme
Maintaining process: - Functions; - Performance; - Security.	According scheme	According scheme Verification Maintenance	Ongoing	According scheme
Management processes: - Quality; - Staff - Corrective actions - Corrective measurements	According scheme	According scheme Verification	Ongoing	According scheme
Measuring and testing equipment - measuring equipment - calibration if applicable				
Information management Confidential Integrity Availability	According scheme	According scheme Verification	Ongoing	According scheme