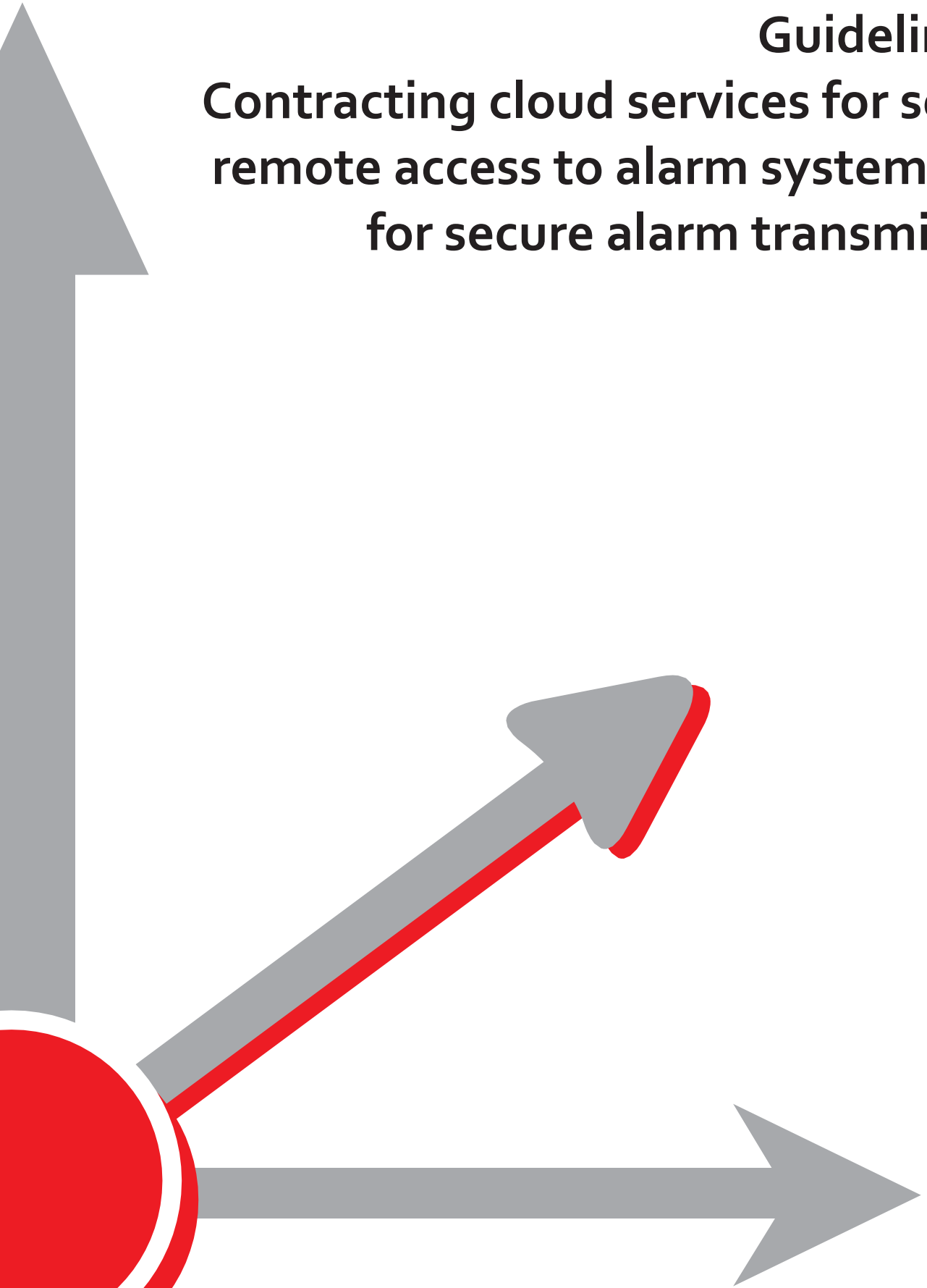
Guideline on Contracting cloud services for secure remote access to alarm systems and for secure alarm transmission



Changes revision table

Date	Rev #	Paragraph /Page	Change
February 2025	1.0		First release

FOREWORD

This document is intended as a general guidance and is not a substitute for detailed advice in specific circumstances. Although great care has been taken in the compilation and preparation of this publication to ensure accuracy, Euralarm cannot in any circumstances accept responsibility for errors, omissions or advice given or for any losses arising from reliance upon information contained in this publication.

DISCLAIMER

This document is intended solely for guidance of Euralarm members, and, where applicable, their members, on the state of affairs concerning its subject. Whilst every effort has been made to ensure its accuracy, readers should not rely upon its completeness or correctness, nor rely on it as legal interpretation. Euralarm will not be liable for the provision of any incorrect or incomplete information.

Note: The English version of this document is the approved Euralarm reference document.

Copyright Euralarm

© 2025, Zug, Switzerland

Euralarm • Gubelstrasse 11 • CH-6300 Zug • Switzerland

E: secretariat@euralarm.org
W: www.euralarm.org

Table of contents

1. Introduction

It is becoming more commonplace to use the latest technology to provide IP-based alarm transmission and remote access to fire safety systems and/or security systems (FSSS) and as such locate part of the equipment outside of the premises of the FSSS service provider. This document will assist FSSS service providers (e.g. installers) when utilising the services of a datacentre to house part of the equipment.

Two different use cases are considered here with their specific requirements and target audience.

- One use case is alarm transmission via an Alarm Transmission System (ATS) operated and managed by an Alarm Transmission Service Provider (ATSP) for which availability, transmission time, fault reporting and protection against substitution are key features. The standard for Alarm Transmission Systems (ATS) EN 50136-1 allows for hosted configurations where the cloud element is required to be in a secure location, which can be a data centre. The highest categories of ATS include security requirements to be fulfilled throughout the whole system. Guidance for this use case is addressed to any entity taking the role of ATSP.
- Another use case is remote access to the FSSS via a Remote Access Infrastructure (RAI) operated and managed by a Remote Access Infrastructure Service Provide (RAISP) for which secured access to the FSSS and data are key features, while availability is for convenience only. The technical specification for the Remote Access Infrastructure (RAI) CLC/TS 50136-10 requires the Remote Access Server (RAS) to be in a secure location and includes requirements for the security of the transferred data. Guidance for this use case is addressed to any entity taking the role of RAISP, more specifically to small and medium FSSS service providers who intend to take the role of RAISP and are not familiar with cloud services and wish to deliver remote services in accordance with EN 50710.

While there are a number of good reasons to consider cloud solutions, FSSS service providers should understand the impact on their business, including availability, service level agreements, data security, compliance, legal & contractual requirements. FSSS service providers will still need to demonstrate compliance with existing standards, e.g. performance & availability, back-ups, access control, etc. The responsibilities for maintenance should be clearly understood and accepted by all stakeholders. These will include life cycle management for operating systems, platforms (e.g. database, virtualisation, etc) and applications. The FSSS service provider should be able to confirm that these activities have been carried out in accordance with the FSSS service providers expectations and service agreements.

The storage, sharing and security of data is vitally important and will need legal consideration over and above what this document states, therefore this document does not attempt to interpret those legal requirements or provide guidance on them.

Significant sections of the present guideline have been taken out of BSIA guidance "ARC considerations when utilising data centre or cloud services" with due acceptance of BSIA. EURALARM is thankful to its member the British Security Industry Association for this contribution.

This guideline provides a description of important concepts related to cloud services, considers relevant Standards and provides an overview of the legal criteria for the choice of the CSP. However, the guideline does not purport to address all legislative requirements of individual countries within Europe. Care should be taken to consider the guideline in the context of any local legislative requirements which take precedence.

2. Abbreviations

AICPA: American Institute of Certified Public Accountants
AMS: Alarm Management System
ANSI: American National Standards Institute
ARC: Alarm Receiving Centre
AS: Alarm System
ATS: Alarm Transmission System
BSIA: British Security Industry Association
CLC: CENELEC
CSP: Cloud Service Provider
EN: European Standard (Norm)
FaaS: Function as a Service
FSSS: Fire Safety Systems and/or Security Systems
IaaS: Infrastructure as a Service
IEC: International Electrotechnical Committee
ISO: International Standardisation Organisation
IT: Information Technology
MARC: Monitoring and Alarm Receiving Centre
PaaS: Platform as a Service
PSTN: Public Switched Telephone Network
RAC: Remote Access Client
RAE: remote Access Endpoint
RAI: Remote Access Infrastructure
RAS: Remote Access Server
RCT: Receiving Centre Transceiver
RCT-A: RCT at the ARC
RCT-H: Hosted RCT
SaaS: Software as a Service
SLA: Service Level Agreement
SOC: System and Organization Controls
SPT: Supervised Premises Transceiver
TIA: Telecommunications Industry Association
TS: Technical Specification

3. Subject matter

This document covers the cloud element of a Remote Access Infrastructure (RAI, used to remotely access to functionalities of the FSSS) and of an Alarm Transmission System (ATS, used to transmit alarms from the FSSS to the Alarm Receiving Centre).

3.1. Remote access to FSSS

In the case of a RAI, this cloud element is identified as the RAS in Figure 1.

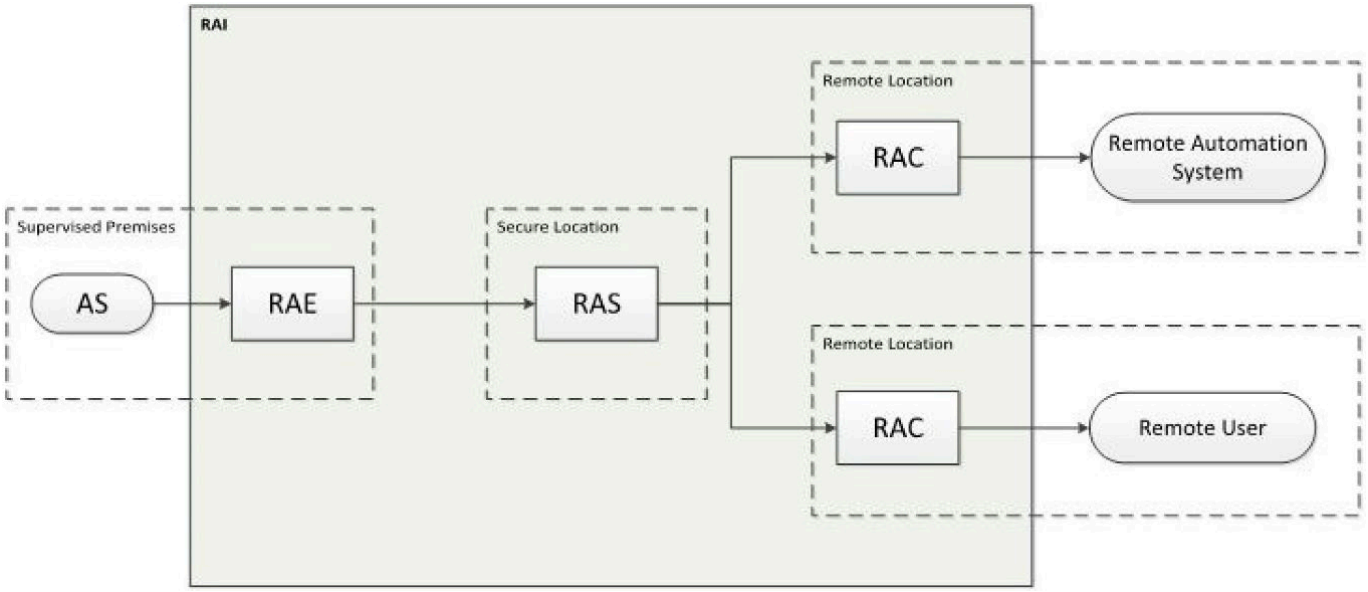


Figure 1. Remote Access Infrastructure logical diagram (taken out of CLC/TS 50136-10:2022)

3.2. Alarm transmission

In the case of an ATS, the European standard allows for a non-hosted configuration depicted in Figure 2a. In this configuration, a direct link is established between the alarm system (AS) and the ARC (MARC). The standard also allows for a hosted configuration depicted in Figure 2b. In this configuration, alarm messages from numerous alarm systems converge to a receiver hosted in a data centre and identified as RCT-H where they are processed, acknowledged and stored and the ARC gets access to them via a secured communication path. Considerations to address the changes from PSTN communications to IP alarm transmission have been given in a Euralarm white paper back in 2019: "New Generation Networks for alarm communications"[1]. The FSSS service provider should ensure that the ATS is compliant with EN 50136-1, the SPT is compliant with EN 50136-2 and the RCT, RCT-H and RCT-A are compliant to EN 50136-3 (see A2.2 in Annex 2 for explanation of those standards). This will ensure that the whole ATS will deliver the alarm messages on time and is monitored for failures to deliver the alarms.

[1] https://www.euralarm.org/resource-report/white-paper-new-generation-networks-for-alarm-communications.html

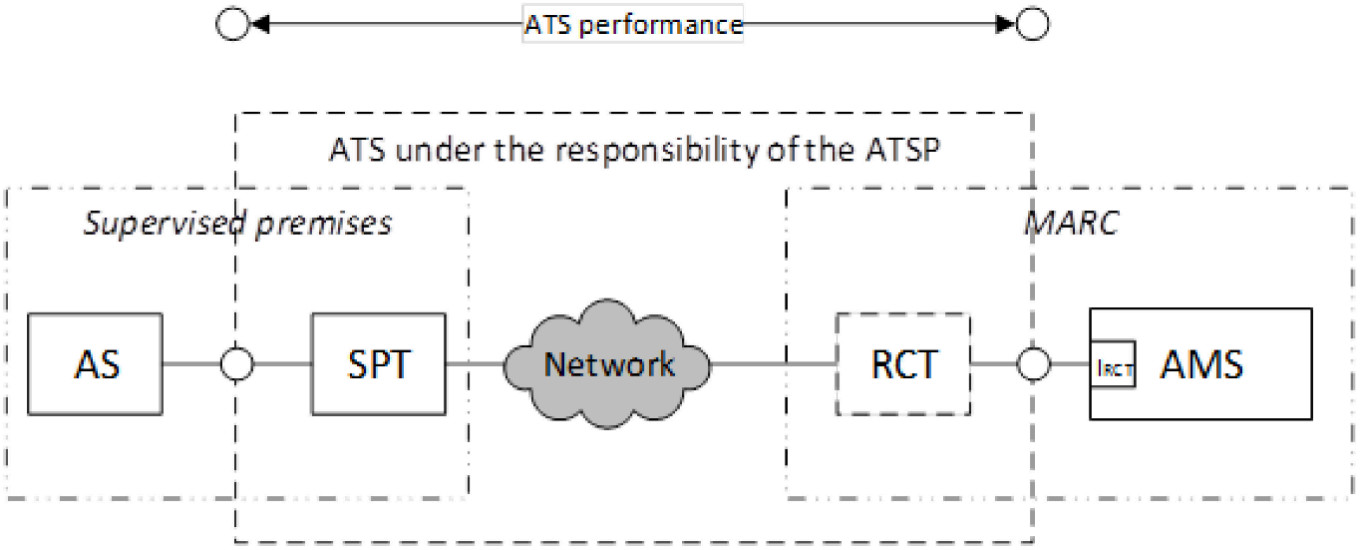


Figure 2a. Example of a **non-hosted** alarm transmission system (taken out of EN 50136-1/A1:2018)

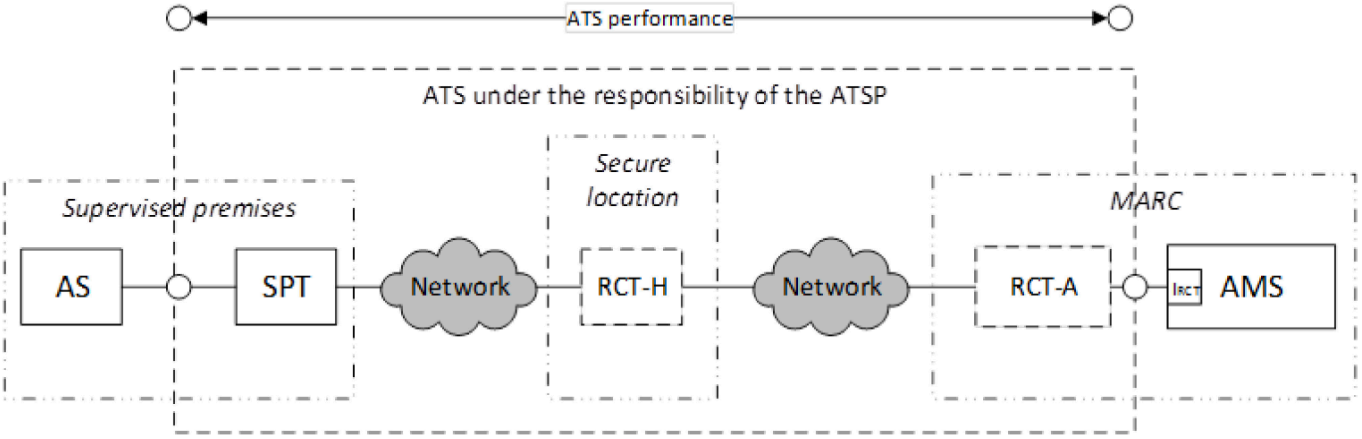


Figure 2b. Example of a **hosted** alarm transmission system (taken out of EN 50136-1/A1:2018)

3.3. General

The present guideline outlines the FSSS service provider considerations when choosing to use the services of a data centre or cloud services. This should assist in deciding how much of the FSSS service provider should/could be safely and securely hosted (or partially hosted) in a cloud environment.

An FSSS service provider is constantly protecting life and property and in this regard the requirements are more critical than most other organisations.

4. Cloud environments

4.1. Introduction

Due diligence is crucial when evaluating and selecting cloud service providers. Due diligence refers to thoroughly researching and assessing potential vendors or service providers before entering into a business relationship with them. This process will assist in better understanding the provider's capabilities, reliability, security measures, and overall suitability for your specific needs.

Three environments are classically defined as: Private business cloud solution, Data Centre Hosted (hereafter Data Centre) or Native Cloud (hereafter Cloud). The FSSS service provider can either use one or more of these environments in which to operate the technical equipment which makes up the remote access or the alarm transmission or use the solution offered by the manufacturer of the FSSS.

This document does not imply that either Private business cloud solutions or Cloud environments are the singular operating mode for all applications, but there is a recognition that the FSSS service provider can and will operate applications in multiple environment models. In other words, they may utilise all three operating environments to lesser or greater degrees, depending on the service requirements.

FSSS service providers should also consider their third-party certification requirements when choosing own solution or data centre or cloud solutions.

The use of data centres/cloud services does not preclude FSSS service provider responsibilities as detailed in EN 16763, EN 50710 or EN 50136-1 (see A2.2 in Annex 2 for explanation of those standards). A Euralarm guidance[2] dedicated to the implementation of remote services has been published and can be found on the website. It helps the FSSS service provider prechecking its compliance with the requirements of these standards.

4.2. Private business cloud solution

Private business solutions are managed by the FSSS service provider. The servers are either installed within the same building or premises where the FSSS service provider is located or in another building under the responsibility of the FSSS service provider. An application provider will supply the service company the software to run on servers. Servers are either procured by the FSSS service provider or purchased as part of the application provider's service.

Upgrades to server operating systems, databases and the application software will be coordinated between the FSSS service provider and Application Provider. Security (encryption at rest etc.) and reliability (such as database replication with geographical diversity) are solutions which are generally built by the application provider.

4.3. Data Centre

Data centre solutions are servers which are installed at a premises operated by a third-party company who provides physical security, power and rack space to house servers. These servers may be dedicated to a specific FSSS service provider or operate a multi-tenant environment. These servers are either maintained by the FSSS service provider or by the application provider as a managed service.

4.4. Cloud

4.4.1. Description

Cloud solutions include all the features of the data centre solution, but the servers and other related technologies (databases etc.) are provided and maintained by the cloud service provider (e.g. AWS - Amazon Web Services, Microsoft Azure, Google Cloud, IBM). The Cloud Shared Responsibility Model (SRM) is a framework that delineates the responsibilities between a cloud service provider and the application provider for securing the

[2] https://www.euralarm.org/resource/guidance-on-remote-services---final-xlsx.html

cloud environment.

The cloud service provider protects the assets of the application developer's environment. For example, they provide physical security and secure the virtualization services. The application provider secures the assets in its cloud instance, i.e. the application provider secures the operating system they install on servers and maintain who has access to your cloud environment.

Cloud computing encompasses several models that cater to different needs and use cases. It is important to note that these models are not mutually exclusive, and cloud service providers often offer a combination of them to cater to different requirements and preferences. The following sections describe 4 different cloud models.

4.4.2. Infrastructure as a Service (IaaS)

This model provides virtualized computing resources over the internet. It offers virtual machines, storage, and networks that users can provision and manage. Users have more control over the infrastructure, including operating systems and applications.

4.4.3. Platform as a Service (PaaS)

PaaS offers a platform for developers to build, deploy, and manage applications without worrying about the underlying infrastructure. It provides a pre-configured environment with tools, frameworks, and runtime for application development. Users can focus on coding and application logic while the platform handles scalability, load balancing, and deployment.

4.4.4. Serverless Computing

Serverless computing is a model where developers write and deploy code as individual functions or units of code. The cloud service provider manages the infrastructure and automatically scales and provisions resources based on demand. Developers do not need to worry about servers or infrastructure management, focusing solely on writing the code.

4.4.5. Software as a Service (SaaS)

SaaS is a complete software application delivered over the internet. End-users of the FSSS or FSSS service providers can access and use the software without the need for installation or management. Providers of SaaS solutions will run their servers in IaaS, PaaS or Serverless computing models.

4.4.6. Considerations for native cloud models

It is important to carefully consider the specific requirements and constraints of a mission-critical application when choosing between environments. Factors such as performance needs, scalability requirements, management options, and cost considerations should be weighed to determine the best fit for the application's objectives.

Refer to Annex 1 for more information.

4.5. Manufacturer solution

Manufacturers of FSSS have developed their solutions and offer them to the FSSS service providers using their systems. Such a solution can be based on either of the 3 environments described above. The FSSS service provider doesn't need to care about the maintenance of the servers, software and application. He needs to ensure a contractual agreement that fits his needs and expectations.

Usually, the FSSS service provider has no contract with the manufacturer for the use of its solution, but he accepts the terms of condition by logging into the application on the cloud. Therefore, it is advised that the manufacturer should make up a document for the installer where he is clear on his cloud application:

- Which cloud service provider,
- where the data will be located,
- how they are accessible including security measures,
- service level like recovery time and maintenance,
- which certification the manufacturer can reference,
- how the FSSS service provider should properly connect the FSSS,
- ...

4.6. Considerations for operating environments

Private business cloud solutions and Data Centre solutions require investment in hardware, software, and infrastructure, and the expertise to set up and maintain them. Cloud based solutions still require the application provider to have the skills to understand, monitor and scale the functionality required. The cloud service provider bundles expert IT services for the deployment and maintenance of the hardware, operating systems and database software.

Steps should be taken to consider the security of data accessible via online or cloud-based connections.

5. Legal criteria for location of servers

5.1. Introduction

Data server regulations in European countries are governed by a combination of national laws and European Union regulations. Here is an overview of the key rules in various European countries, as well as the overarching EU framework.

5.2. European Union General Data Protection Regulation (GDPR)

The GDPR, effective since May 2018, is the primary regulation governing data protection and privacy in the EU. It applies to all member states and includes:

- data processing principles: lawfulness, fairness, transparency, purpose limitation, data minimization, accuracy, storage limitation, integrity, and confidentiality;
- data subject rights: right to access, rectification, erasure (right to be forgotten), restriction of processing, data portability, and objection;
- data transfer: restrictions on transferring personal data outside the EU/EEA, ensuring adequate levels of protection;
- data breach notifications: obligation to notify authorities and affected individuals of data breaches within 72 hours.

5.3. Examples of Country-Specific Regulations

Germany

Federal Data Protection Act (Bundesdatenschutzgesetz, BDSG): Supplements the GDPR with additional requirements, including stricter rules on data processing for employment purposes and specific obligations for data protection officers.

France

Data Protection Act (Loi Informatique et Libertés): Enforces GDPR provisions and adds national specifics, such as rules on the processing of health data and additional powers for the national data protection authority (CNIL).

United Kingdom

Data Protection Act 2018: Implements GDPR and includes specific provisions for data processing by public authorities and law enforcement agencies. Following Brexit, the UK has adopted the UK GDPR, which mirrors the EU GDPR but operates independently.

Italy

Data Protection Code (Codice in materia di protezione dei dati personali): Aligns with GDPR, with additional national rules on data processing for scientific and historical research, and journalistic purposes.

Spain

Organic Law on Data Protection and Digital Rights (LOPDGDD): Complements GDPR with specific rules on digital rights and additional protections for minors and vulnerable individuals.

Netherlands

Dutch Implementation Act (Uitvoeringswet AVG): Supplements GDPR with national provisions, particularly concerning the processing of criminal records and employee data.

Belgium

Belgian implementation law (Gegevensbeschermingsautoriteit GBA) framework law of 30 july 2018

The common themes across countries are:

- data localization: some countries have specific requirements for data localization, particularly for sensitive data such as health records;
- sector-specific regulations: many countries impose additional regulations for certain sectors, like finance, health, and telecommunications;
- Data Protection Authorities (DPAs): each country has a national DPA responsible for enforcing data protection laws and handling complaints. Examples include CNIL in France, ICO in the UK, and BfDI in Germany;
- cross-border data transfers: EU countries generally follow the GDPR's framework for international data transfers, which include mechanisms like Standard Contractual Clauses (SCCs), Binding Corporate Rules (BCRs), and adequacy decisions.

This list of country-specific legislations is not exhaustive. For more specific regulations and the latest updates, it's advisable to consult the respective national DPAs and legal texts in each country.

5.4. Useful references

- European Commission - Data Protection[3]
- GDPR Text[4]
- CNIL (France)[5]
- ICO (UK)[6]
- BfDI (Germany)

6. Distributions of roles and responsibilities

6.1. Impact of maintenance activities (planned/unplanned)

Availability of the infrastructure can be of different criticality depending on the services delivered with it. Alarm transmission services require a high availability defined by the applicable category out of EN 50136-1. Availability is generally considered as less critical for remote access services.

The FSSS service provider (or the manufacturer in the Manufacturer solution environment) should have processes in place for how maintenance activities will be managed and where necessary mitigated, e.g. secondary system availability or duplicated infrastructure etc.

FSSS service providers considering a hosted solution should ensure that agreements (SLAs) are in place with the cloud service providers to ensure that the FSSS service provider is notified in advance of the duration of off-line periods during planned maintenance. These agreements should also include how unplanned maintenance is managed and communicated.

Where FSSS service providers are relying on 3rd parties for IT services, then the FSSS service provider should consider how incidents may impact the IT service providers ability to provide support.

6.2. IT competence

The FSSS service provider is ultimately responsible for their own equipment and systems and will require some level of local IT competence to ensure that routine monitoring and maintenance activities on the FSSS service provider solution are managed.

6.3. Security

FSSS service providers should consider who has access to their systems, data and consider staff screening requirements. There are several options to solve security challenges, including:

- Identity and access management (IAM)
- Encryption
- Security monitoring and logging
- Compliance and certifications
- Network security.

[3] https://commission.europa.eu/law/law-topic/data-protection_en
[4] https://eur-lex.europa.eu/eli/reg/2016/679/oj
[5] https://www.cnil.fr/en
[6] https://ico.org.uk

Data centre solutions require on prem staff and/or remote access to manage and maintain the infrastructure, including hardware maintenance, software upgrades, and security patches. In contrast, cloud solutions are managed by the cloud service provider, which handles all infrastructure maintenance, software upgrades, and security patches, freeing up internal IT staff to focus on core business functions.

In any cloud environment, there's a shared responsibility between the Cloud Service Provider (CSP) and the user (FSSS service provider or manufacturer). Security for things like data classification, network controls, and physical security need clear owners. The division of these responsibilities is known as the shared responsibility model (SRM) for cloud security. Check out this chart to see where the responsibilities lie within different cloud environments.

Private business cloud solution	**Infrastructure as a Service *IaaS***	**Platform as a Service *PaaS***	**Software as a Service *SaaS***
Data & Configurations	Data & Configurations	Data & Configurations	Data & Configurations
Application Code	Application Code	Application Code	Application Code
Scaling	Scaling	Scaling	Scaling
Runtime	Runtime	Runtime	Runtime
Operating System	Operating System	Operating System	Operating System
Virtualisation	Virtualisation	Virtualisation	Virtualisation
Hardware	Hardware	Hardware	Hardware
Managed by FSSS service provider or manufacturer			
Managed by cloud service provider			

Further information and guidance about SRM can be found on the website of the Center for Internet Security (CIS)[7].

7. Contracting cloud services

The European Commission wrote back in 2012 in their Communication entitled "Unleashing the potential of cloud computing in Europe"[8]:

> *"Traditional IT outsourcing arrangements were typically negotiated and related to data storage, processing facilities and services defined and described in detail and up-front. Cloud computing contracts, on the other hand, essentially create a framework in which the user has access to infinitely scalable and flexible IT capabilities according to his needs. However, currently the greater flexibility of cloud computing as compared to traditional outsourcing is often counterbalanced by reduced certainty for the customer due to insufficiently specific and balanced contracts with cloud providers.*
>
> *The complexity and uncertainty of the legal framework for cloud services providers means that they often use complex contracts or service level agreements with extensive disclaimers. The use of "take-it-or-leave-it" standard contracts might be cost-saving for the provider but is often undesirable for the user, including the final consumer. Such contracts may also impose the choice of applicable law or inhibit data recovery. Even larger companies have little negotiation power and contracts often do not provide for liability for data integrity, confidentiality or service*

[7] https://www.cisecurity.org/insights/blog/shared-responsibility-cloud-security-what-you-need-to-know
[8] https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0529:FIN:EN:PDF

continuity."

In order to help tackling this complexity and uncertainty, detailed guidance on key contractual elements can be found in the "Guidelines on outsourcing to cloud service providers"[9] issued by the European Securities and Markets Authority (esma) in 2021 in numerous European languages. In particular, the following sections of the document can be relevant:

- Guideline 3 – Key contractual elements
- Guideline 4 – Information security
- Guideline 5 – Exit strategies
- Guideline 6 – Access and Audit Rights.

NOTE: similar guidance can also be found on the website of the European Insurance and Occupational Pensions Authority (eiopa)[10].

In addition, in the frame of the Data Act ((EU) 2023/2854), the European Commission is preparing standard contractual clauses to guide the stakeholders with the implementation of the provisions regarding the switching of cloud service provider and the share of data. This guidance is expected to be published in the course of 2025.

Finally, Annex 2 of this Euralarm guideline provides reference to standards and certification schemes to which compliance can be required in the contract with the cloud service provider.

More information on cloud computing contracts can be found on EC website:

- "Cloud computing contracts"[11]
- "Comparative study on cloud computing contracts"[12]

8. Conclusion

Since there is neither unique nor unified certification scheme for data centres and cloud services, the FSSS service provider should be assured that the CSP makes sure that the data centre meets the needed reliability and security requirements for the considered use case. Any compliance statement claimed by the CSP or manufacturer to demonstrate the reliability and security of the cloud service should at least encompass the following considerations:

- regarding the used data centre:
  - its name and location(s);
  - level of business continuity assurance from no continuity to full continuity in case of data centre failure (critical for alarm transmission and convenience for remote access);
  - means to minimise the risk of failure like single or multiple site(s) selection, building structure, power systems, cooling systems, mechanical systems, architecture, physical security, cybersecurity, cabling infrastructure, telecommunications systems, back-up policy, fire protection, and safety (critical for alarm transmission and convenience for remote access);

[9] https://www.esma.europa.eu/document/guidelines-outsourcing-cloud-service-providers
[10] https://www.eiopa.europa.eu/system/files/2020-04/guidelines_on_outsourcing_to_cloud_service_providers_en.pdf
[11] https://commission.europa.eu/business-economy-euro/doing-business-eu/contract-rules/cloud-computing/cloud-computing-contracts_en
[12] https://op.europa.eu/en/publication-detail/-/publication/40148ba1-1784-4d1a-bb64-334ac3df22c7

- regarding the cloud service:
    - used cloud environment;
    - clear and understood distribution of roles and responsibilities properly laid down in a SLA;
    - Disaster Recovery Plan (DRP) in place (critical for alarm transmission and convenience for remote access);
    - test plan after a software update;
    - notification of the FSSS service provider in case of system updates, software updates, or change of providers;
- regarding cybersecurity and privacy of data centre and cloud service:
    - compliance to ISO/IEC 27001;
    - certificate under the EUCS certification scheme (when available, see A2.6);
    - secure access control mechanisms with authentication to access stored data and functions;
    - encryption of data in transit;
    - mitigation of the effects of (D)DOS attacks;
    - vulnerability handling process;
    - verification via penetration testing;
- for alarm transmission:
    - compliance of the ATS to EN 50136-1 at a declared category that is appropriate to the protected risk (transmission time, availability, reporting time in case of failures to transmit, encryption requirement, substitution security, mode of acknowledgement etc.);
    - dual path (DP) category where high risks are covered or for vital (life-threatening) systems;
- for remote access to FSSS:
    - compliance of the RAI to CLC/TS 50136-10.

9. Bibliography

"ARC considerations when utilising data centre or cloud services", BSIA (British Security Industry Association), Issue 1, October 2023.

Annex 1 - Data Centre/IaaS and Serverless

For a mission-critical application, both IaaS (Infrastructure as a Service) and serverless environments have their pros and cons. Here are some comparisons between the two:

- Management Complexity: In an IaaS environment, users have full control over the infrastructure, which means they need to handle tasks like provisioning and managing servers, configuring networking, and ensuring high availability. This requires more expertise, time, and resources compared to a Serverless environment where infrastructure management is abstracted away. With Serverless, application providers can focus solely on delivering software services, but they have less understanding of the underlying infrastructure, which may be a limitation for certain mission-critical applications.

- Scalability: In an IaaS environment, scaling infrastructure to handle increased traffic or demand requires manual intervention and configuration. On the other hand, serverless environments automatically scale resources based on the number of requests or events triggered, allowing for more dynamic scalability. However, serverless may have certain limitations on scalability, such as maximum concurrent executions or execution duration, which can impact highly demanding applications.

- Cold Start and Performance: Serverless environments often have a concept called "cold start," where the first execution of a function incurs additional latency due to the need to initialize the runtime environment. This latency can impact real-time or low-latency applications. In an IaaS environment, applications run on dedicated servers or virtual machines, which typically offer consistent performance without cold start delays. Additionally, serverless environments may have limitations on resources allocated to individual functions, which can affect the performance of resource-intensive applications.

- Vendor Lock-In: While both IaaS and serverless environments involve some level of vendor lock-in, serverless environments often have more tightly integrated services and event-driven architectures, which can make it more challenging to migrate applications across different cloud service providers or to on-premises infrastructure. In an IaaS environment, users have more flexibility to move their applications between different providers or even bring them in-house.

- Cost and Predictability: Serverless environments follow a pay-per-use pricing model, which can be cost-effective for applications with sporadic or variable workloads. However, the pricing structure can sometimes be complex and unpredictable, especially with additional charges for API calls, data transfer, and resource usage. In an IaaS environment, users have more control over resource allocation and pricing, allowing for better cost predictability but potentially higher fixed costs.

Annex 2 - Standards and certification schemes

A2.1. Introduction

The following are core standards relating to alarm transmission, remote access and data centres which might be useful when determining the performance of a system or service in terms of its resilience, robustness and reliability.

A2.2. Standards for alarm transmission, remote access to alarm systems and remote services

EN 50136-1 General requirements for alarm transmission systems

This European Standard specifies the requirements for the performance, reliability and security characteristics of alarm transmission systems. It specifies the requirements for alarm transmission systems providing alarm transmission between an alarm system at a supervised premises and annunciation equipment at an alarm receiving centre.

This European Standard applies to transmission systems for all types of alarm messages such as fire, intrusion, access control, social alarm, etc.

A FSSS service provider taking the role of ATSP (Alarm Transmission Service Provider) should be compliant with the provisions of this standard.

CLC/TS 50136-10 Alarm systems - Requirements for remote access

This document specifies minimum requirements for secure connection and session for remote access to one or more alarm systems, for example fire safety systems, intruder and hold-up alarm systems, electronic access control systems, external perimeter security systems, video surveillance systems, and social alarm systems.

This document specifies the requirements for the performance, reliability, integrity, and security characteristics of a Remote Access Infrastructure.

This document specifies the requirements for a Remote Access Infrastructure between a Remote Access Client and an alarm system at the supervised premises and may be either integrated as part of the ATS or a separate infrastructure.

A FSSS service provider taking the role of RAISP (Remote Access Infrastructure Service Provider) should be compliant with the provisions of this technical specification.

EN 50710 Requirements for the provision of secure remote services for fire safety systems and security systems

This document specifies the minimum requirements for the provision of secure remote services via a remote access infrastructure (RAI) carried out either at site or off-site (e.g. via IP connections) to the following systems:

a) fire safety systems including, but not limited to, fire detection and fire alarm systems, fixed firefighting systems, smoke and heat control systems;
b) security systems including, but not limited to, intruder and hold-up alarm systems, electronic access control systems, external perimeter security systems and video surveillance systems;
c) social alarm systems;
d) emergency sound systems;
e) a combination of such systems;
f) management systems connected to systems a) – e).

This standard is intended to complement EN 16763 *Services for fire safety systems and security systems.*

A2.3. Standard for cloud services

CEN/TS 18026 Three-level approach for a set of cybersecurity requirements for cloud services

This Technical Specification (TS) provides a set of cybersecurity requirements for cloud services. This TS is applicable to organizations providing cloud services and their subservice organizations.

Note: this new TS is expected to be published during summer 2024.

A2.4. Standard for information security management systems

ISO/IEC 27001 Information security, cybersecurity and privacy protection - Information security management systems - Requirements

ISO/IEC 27001 is a widely recognized international standard that outlines the best practices for implementing and maintaining an Information Security Management System (ISMS). This standard provides a framework for the management of information security risks, including people, processes, and technology.

ISO/IEC 27001 covers all aspects of information security, including confidentiality, integrity, and availability, and it requires organizations to implement controls to ensure the confidentiality, integrity, and availability of their information assets.

The standard also requires organizations to adopt a risk-based approach to information security management, which involves identifying and assessing risks, implementing appropriate controls to mitigate those risks, and continuously monitoring and reviewing the effectiveness of the controls.

By implementing ISO/IEC 27001, organizations can demonstrate their commitment to information security and provide assurance to stakeholders that their information assets are being managed in a secure and effective manner. The standard is applicable to organizations of all sizes and industries, and it is widely recognized as a benchmark for information security management.

A2.5. Standards for data centres

ISO/IEC 22237 (and EN 50600) Information technology - Data centre facilities and infrastructures

ISO 22237 is the ISO standard series that governs the design, structure, operation, physical and information

security of data centres. The intention of the standard is to define the necessary conditions to allow the objectives of ISO 27001 to be achieved in a data centre environment.

The EN 50600 is the EN standard series that provides for the planning, design, procurement, integration, installation, operation and maintenance of facilities and infrastructures within data centres. Whilst the EN 50600 series provides similar provisions to the ISO 22237 standards, they are not fully aligned.

EN 50600 is a growing family of standards currently made of the following parts:

- EN 50600-1, General concepts
- EN 50600-2-1, Building construction
- EN 50600-2-2, Power supply and distribution
- EN 50600-2-3. Environmental control
- EN 50600-2-4, Telecommunications cabling infrastructure
- EN 50600-2-5, Security systems
- EN 50600-3-1, Management and operational information
- EN 50600-4-1, Overview of and general requirements for key performance indicators
- EN 50600-4-2, Power Usage Effectiveness
- EN 50600-4-3, Renewable Energy Factor

EN 50600 provides for a classification system based upon the key criteria of availability, security and energy efficiency:

1. Availability Class. AC classification is defined in the areas of power supply, ventilation and air-conditioning systems and cabling;
2. Protection Class. PC is defined for intrusion prevention, fire protection, smoke protection as well as protection against environmental hazards. At least three protection classes are to be formed;
3. Granularity Level (GL). The capability for energy-efficient operation is defined by means of measurement qualities and measurement scope for the ventilation and air-conditioning systems. The standard differentiates between three different granularity levels;

For a data centre design to conform to this standard:

a. A business risk analysis shall be completed;
b. An appropriate AC class shall be selected using the business risk analysis;
c. An appropriate PC for the data centre pathways and spaces;
d. An appropriate energy efficiency enablement level, GL;
e. The design process and principles shall be applied.

Note: Currently, data centres are usually not considering neither EN 50600 nor ISO 22237. Data centres (AWS, …) are generally certified by the private Uptime Institute (Tier Certification) and/or according to ANSI/TIA-942. These 2 certifications schemes are considered as complementary.

Uptime Institute Tier Certification

This private certification body apply their own Tier Standards for data center availability and overall performance. It allows for various performance levels that consider both the built environment, as well as the approach and performance of the operations team. 4 levels are defined:

- Tier I: Basic Capacity: Site-wide shutdowns are required for maintenance or repair work. Capacity or distribution failures will impact the site..
- Tier II: Redundant Capacity Components: Site-wide shutdowns for maintenance are still required.

Capacity failures may impact the site. Distribution failures will impact the site.

- Tier III: Concurrently Maintainable: Each and every capacity component and distribution path in a site can be removed on a planned basis for maintenance or replacement without impacting operations. The site is still exposed to an equipment failure or operator error.
- Tier IV: Fault Tolerant: An individual equipment failure or distribution path interruption will not impact operations. A Fault Tolerant site is also Concurrently Maintainable.

ANSI/TIA-942 Telecommunications Infrastructure Standard for Data Centers

ANSI/TIA-942 is a standard published by the Telecommunications Industry Association (TIA) that provides guidelines for the design and construction of data centres, including power systems, mechanical systems, architecture, security, telecommunications systems, fire protection, and safety. The standard is intended to ensure that data centres are reliable, secure, and scalable to meet the evolving needs of the IT industry.

ANSI/TIA-942 provides a comprehensive framework for data centre design, including recommendations for site selection, building structure, cabling infrastructure, cooling and power systems, security, and management.

ANSI/TIA-942 is used by data centre designers, operators, and auditors to ensure that data centres are designed and built to meet industry best practices and standards. The standard is also frequently referenced by regulatory bodies and customers to evaluate the reliability and security of data centres.

System and Organization Controls (SOC) 2

SOC 2 is a set of standards developed by the American Institute of Certified Public Accountants (AICPA) to assess and audit the security, availability, processing integrity, confidentiality, and privacy of a service organization's systems and data.

Note: while ISO/IEC 27001 is generic, SOC 2 is contextualised for data centres.

SOC 2 reports are used by service organizations (such as data centres) to demonstrate to their customers and stakeholders that they have effective internal controls in place to protect their sensitive data.

SOC 2 reports are based on the Trust Services Criteria (TSC), which is a set of principles and criteria used to evaluate the effectiveness of a service organization's controls over its systems and data.

There are two types of SOC 2 reports: Type I and Type II. Type I reports evaluate the design of a service organization's controls, while Type II reports evaluate the effectiveness of those controls over a specified period.

SOC 2 audits are conducted by independent third-party auditors, who are certified by the AICPA.

SOC 2 audits are voluntary, but they are becoming increasingly important for service organizations that want to demonstrate their commitment to security and privacy.

To prepare for a SOC 2 audit, service organizations must conduct a risk assessment and implement a comprehensive set of controls to address the Trust Services Criteria.

SOC 2 audits typically involve a combination of interviews, documentation reviews, and system testing to evaluate the effectiveness of a service organization's controls.

SOC 2 reports include an opinion from the auditor on the effectiveness of a service organization's controls, as well as a description of the controls that were tested and any identified deficiencies.

SOC 2 reports can be shared with customers, stakeholders, and regulatory bodies to provide assurance that a service organization has implemented effective controls to protect sensitive data.

Is SOC 2 report Type II THE recommendation for cybersecurity aspects?

SOC 3

SOC iii is a type of attestation report that provides a high-level overview of an organization's controls related to security, availability, processing integrity, confidentiality, and privacy.

Unlike SOC 1 and SOC 2 reports, which are intended for a specific audience and provide more detailed information about an organization's controls, SOC 3 reports are designed for a general audience and provide a summary of the organization's controls that can be publicly shared.

SOC 3 reports are based on the same controls and criteria as SOC 2 reports, but they do not provide the same level of detail. Instead, SOC 3 reports include a brief description of the organization's system and controls, along with a statement from an independent auditor attesting to the organization's compliance with the SOC 2 criteria.

SOC 3 reports are often used by organizations to demonstrate their commitment to security and compliance to customers, partners, and other stakeholders. Because they are publicly available, they can also be used by potential customers or investors to evaluate an organization's security posture before doing business with them.

A2.6. Certification schemes

The Cyber Security Act (CSA, (EU) 2019/881) provides a European framework for the cybersecurity certification of products, processes and services. ENISA, the European union agency for cybersecurity, is entitled to develop cybersecurity certification schemes intended to be used on a voluntary basis and valid across the whole European Union. The second scheme intends to cover Cloud Services (EUCS). It is still under preparation at the date of writing the present guidance. This scheme is expected to make use of the CEN/TS 18026 presented above. When available, it could become a useful tool for the CSP's to demonstrate the security of his solution and for the FSSS service provider to trust the CSP.

Publication date: 14-02-205

Euralarm
Gubelstrasse 22
CH-6301 Zug (Switzerland)

Swiss Commercial Registration No: CHE-222.522.503

E secretariat@euralarm.org
W www.euralarm.org