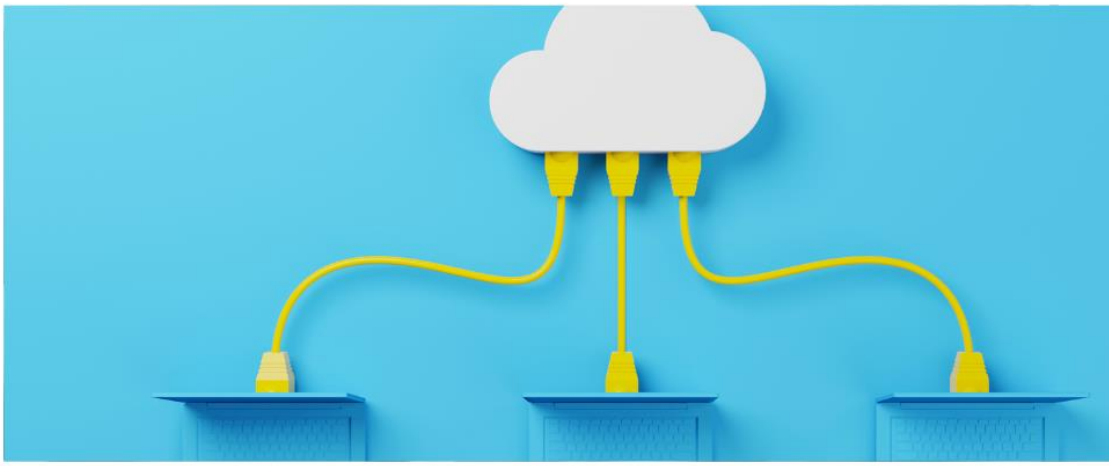


ARC considerations when utilising **data centre or cloud services**

Contents

1. Introduction

It is becoming more commonplace to use the latest technology to provide ARC services and as such locate ARC equipment outside of the ARC shell. This document will assist ARC operators when utilising the services of a datacentre to house ARC equipment.

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.

The current ARC standard EN 50518:2019+A1:2023 specifies where key ARC equipment (as listed in EN 50518) should be located. Where ARC equipment is not located within the ARC shell, the standard provides 2 additional options.

a) Within the same building or premises as the ARC and built to the same requirements of the ARC shell or another compliant ARC.
b) A “secure location”, defined in paragraph 3.1.36 to include “another location that complies with a published data centre standard”.

In addition, EN 50518 also specifies the performance requirements of links between the ARC and the remote location. i.e. meeting the requirement of the signalling standard EN 50136:2012 +A1:2018 category DP4. This describes security, availability and general performance criteria.

ARCs will have seen an increase in the number of hosted services they provide to their customers, e.g. IP Signalling and hosted Video Surveillance Systems (VSS) related services.

Application developers are also considering the benefits of moving to SaaS (Software as a Service - cloud hosted solutions) models to provide options to ARCs.

While there are a number of good reasons to consider cloud solutions, ARCs should understand the impact on their business including, availability, SLA’s, data security, compliance, legal & contractual requirements. ARCs 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 ARC should be able to confirm that these activities have been carried out in accordance with the ARCs expectations and service agreements.

2. Scope

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

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

3. Terms and abbreviations

ARC	Alarm Receiving Centre (this also includes Remote Video Receiving Centres (RVRCs) in this document)
Data Centre	Data Centre Hosted (Equipment located outside the shell of the ARC)
Cloud	Native Cloud (EG: AWS - Amazon Web Services, Microsoft Azure, Google Cloud, IBM).
On Prem	On Premises (Equipment located within the shell of the ARC)
SLA	Service Level Agreement

4. Considerations

4.1. General

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.

The EN 50518 Alarm Receiving Centre (ARC) Standard allows ARCs to use one or more of three environments in which to operate the technical equipment which makes up “Alarm Receiving” and “Alarm Management”. These generic terms are used in this document to include applications such as Intruder, Fire and Video Monitoring, Fault Reporting and AI applications. Some of these applications may naturally operate as “On Premises” solutions and some will be better suited, or are dependent, on cloud infrastructure and services.

This document does not imply that either On Premises or Cloud environments are the singular operating mode for all applications, but there is a recognition that ARCs 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 ARC requirements.

The three environments are On Premises (hereafter On Prem), Data Centre Hosted (hereafter Data Centre) or Native Cloud (hereafter Cloud).

ARCs should also consider their third-party certification requirements when choosing on prem or data centre or cloud solutions.

The use of data centres/cloud services does not preclude ARC responsibilities as detailed in EN 50518 clauses 5.8.1.1 and 9.1.

4.1.1. On Prem

On Prem solutions are installed within the same building or premises where the ARC is located. An application provider will supply the ARC the software to run on servers. Servers are either procured by the ARC or purchased as part of the application provider’s service.

Upgrades to server operating systems, databases and the application software will be co-ordinated between the ARC 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.

4.1.2. 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 ARC or operate a multi-tenant environment. These servers are either maintained by the ARC or by the application provider as a managed service.

4.1.3. Cloud

Cloud solutions include all the of the data centre solution, but the servers and other related technologies (databases etc.) are provided and maintained by the cloud service provider. 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 cloud environment.

The cloud 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.

4.2. Cloud computing

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 providers often offer a combination of them to cater to different requirements and preferences.

- **Data Centre Hosted:** Data centre hosting is a model where organizations or individuals lease physical space within a data centre facility to house their servers and IT infrastructure. In this scenario, the user takes responsibility for managing and maintaining their servers, operating systems, networking equipment, and other related components.
- **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.
- **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.
- **Serverless Computing:** Serverless computing is a model where developers write and deploy code as individual functions or units of code. The cloud 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.
- **Software as a Service (SaaS):** SaaS is a complete software application delivered over the internet. Users 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.

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.

4.3. Deployment

On Prem 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 provider bundles expert IT services for the deployment and maintenance of the hardware, operating systems and database software.

4.4. Firewall Management

Monitoring centres receiving IP signalling will need to have arrangements for managing firewalls, so that new transmission devices can have their IP protocols configured on the firewall. Consideration should be given to the IT services and response times available to the ARC for setting the firewall rules, whether this is done at the ARC for on prem systems or at the data centre for hosted platforms.

Note: *The ARC may have little notice of the intention of an installing company to transmit from a new type of device, and will therefore need a responsive firewall configuration service, e.g. changes to signalling protocols.*

4.5. Impact of maintenance activities (planned /unplanned)

The ARC 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.

ARCs considering a hosted solution should ensure that agreements (SLAs) are in place with service providers to ensure that the ARC 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 ARCs are relying on 3rd parties for IT services, then the ARC should consider how incidents may impact the service providers ability to provide support.

4.6. IT Competence

The ARC 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 ARC solution are managed.

4.7. Security

ARCs 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

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.

4.8. Telephony Connections

Data centres may not accept exchange line connections to your hosted system and may limit external data links to IP only. This will not be a consideration in the UK in the future as there will be neither PSTN nor ISDN exchange lines supported in the telephone network.

5. Data centre standards

The following are core standards relating to data centres which might be useful when determining the performance of a data centre in terms of its resilience, robustness and reliability.

5.1. ISO 27001 summary

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.

5.2. ISO 22237 summary

ISO 22237 is the ISO standard that governs the design, structure, operation, physical and information security of data centres. It is a direct replacement for ISO EN 50600 comprising 7 sections and is currently in the committee review stage. 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.

5.3. ANSI/TIA-942 summary

ANSI/TIA-942 is a standard published by the Telecommunications Industry Association (TIA) that provides guidelines for the design and construction of data centres. 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. The standard includes four tiers of data centre design, each with increasing levels of redundancy and fault tolerance:

- Tier 1: Basic data centre with a single path for power and cooling, providing 99.671% availability.
- Tier 2: Redundant components with a single path for power and cooling, providing 99.741% availability.
- Tier 3: Redundant components with multiple paths for power and cooling, providing 99.982% availability.
- Tier 4: Fault-tolerant components with multiple paths for power and cooling, providing 99.995% availability.

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.

5.4. System and Organization Controls (SOC) ii summary

SOC ii 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.

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

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

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

SOC ii 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 ii 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.

5.5. SOC iii summary

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

SOC iii reports are based on the same controls and criteria as SOC ii reports, but they do not provide the same level of detail. Instead, SOC iii 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 ii criteria.

SOC iii 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.

6. Legal and other considerations

6.1. Data protection and sovereignty

The cloud providers should be capable of fulfilling data protection obligations.

The cloud provider's approach to data sovereignty, which refers to the legal and regulatory requirements surrounding the storage and processing of data in specific jurisdictions.

6.2. Cyber Security

The cloud provider's physical security practices, incident response protocols, cyber security and certifications such as ISO 27001, Cyber Essentials and ISO 22237 series.

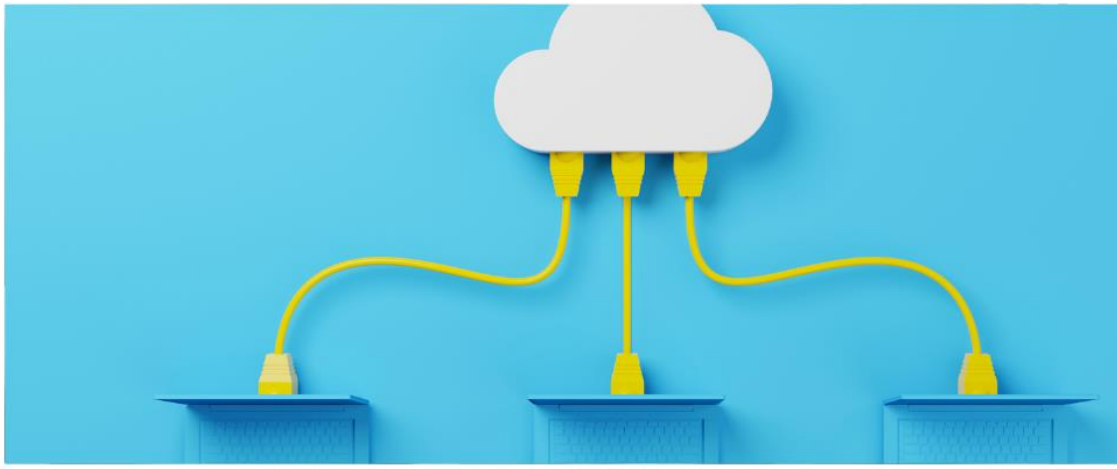
6.3. Cross Border Privacy Rules

The APEC Cross-Border Privacy Rules (CBPR) System, endorsed by the Asia-Pacific Economic Cooperation (APEC) in 2004, is a voluntary, enforceable, international, accountability-based system that facilitates privacy-respecting data flows among APEC economies. CBPR provides a standard set of principles designed to enhance electronic performance, facilitate trade and economic growth, and strengthen consumer privacy protections. There may be others depending on the jurisdiction.

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 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.



About **the BSIA**

The British Security Industry Association (BSIA) is the trade association representing over 70% of the UK's private security industry. Its membership includes companies specialising in all sectors of security. For security buyers, BSIA membership is an assurance of quality, with all member companies required to adhere to strict quality standards.

This guidance has been produced by the Alarm Receiving Centres Section of the BSIA.