EBU

OPERATING EUROVISION AND EURORADIO

R 146

CLOUD SECURITY FOR MEDIA COMPANIES

RECOMMENDATION

SOURCE: SP-MCS

Geneva
September 2017

There are blank pages throughout this document. This document is paginated for two sided printing

Cloud Security for Media Companies

EBU Committee	*First Issued*	*Revised*	*Re-issued*
MCS	2017		

Keywords Information Security, Cybersecurity, IT Security, Cyberattack, Cloud, Cloud Security, Cloud Architecture, Cloud Customer, EBU R143, EBU R144.

Recommendation

The EBU, considering that:

1. Media companies increasingly rely on information technologies and networks;
2. The threat of cyberattacks is growing (and several broadcast companies have been successfully attacked);
3. Adoption of cloud services by media companies changes their overall architecture and workflows, leading to new threats such as their cloud services becoming single points of failure; and
4. Companies have already been attacked from compromised cloud services.

Recommends[1] that:

1. Media companies considering the adoption of cloud services (as a Cloud Customer) shall follow a communicated and accepted cloud adoption procedure that should be embedded into the corporate risk and enterprise strategy;
2. Media companies should achieve a minimum Cybersecurity Maturity Level of three, as set out in EBU R144;
3. Media companies should adopt the minimum baseline security recommended by EBU R143 when deploying systems, software or services to the cloud;

And in particular, the following steps should be part of the cloud adoption procedure:

4. Definition of the objectives of cloud service usage (e.g. functionality, flexibility, costs, service replacement).
5. Determine all related processes, services, systems and data.
6. Conduct a data classification (as described in Annex D) for the data being processed by the Cloud Service Provider as well as the related systems and services.
7. Determine the regulatory framework and possible limitations of cloud service usage according to local and European laws (e.g. data privacy according to EU GDPR[2], procurement

[1] These EBU recommendations are based on cloud best practices provided by different Cloud Service Providers and on national cloud guidelines.

[2] http://www.eugdpr.org/

regulations). Special local regulations such as those concerning the protection of journalist sources should be examined too.

8. Determine the technical and organizational framework (e.g. needed service levels, performance, internet bandwidth and local staff).

9. Determine the corporate acceptance for self-service models.

10. Provide a consistent way for calculating total cost of ownership for cloud service usage.

11. Provide a structured way for analyzing cloud service requirements and for choosing the appropriate Cloud Service Architecture, including all necessary Cloud Security Features described in Annex B.

12. Determine the security requirements for the cloud service, based on corporate security standards and data classification (Annex D). If there are no internal standards available, use well known recommendations of accepted sites (e.g. Cloud Security Alliance or national cybersecurity authorities).

13. Provide a consistent practice for Cloud Service Provider Assessment (see Annex C).

14. Perform a final risk analysis and decide how to treat the remaining risks. The risk analysis should be embedded into the corporate risk management.

15. Provide a standardized workflow for establishing a corporate cloud service usage (see Annex A for a recommended example). This workflow shall also cover end-of-life and Business Continuity Management (BCM) aspects for cloud service usage.

16. Retain backup restore capabilities of important stored data in a fault domain in case of major failures of the Cloud Service Provider.

17. Include tools and mechanisms to manage cloud services and assessed Cloud Service Providers

Four informative Annexes follow.

Annex A: Workflow for establishing a corporate cloud service usage

Definition of Cloud Computing

> According to the NIST special publication 800-145, "*Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.*"

This annex provides a recommended example workflow for adopting a cloud service, starting from an initial user request by the business owner:

(An optional Step might be to centralize all requests at the Procurement Department if budgets are centralized. This can prevent users from buying cloud services by themselves. Normally the workflow would start at Step I.)

- **Step 0a:** The business owner should conduct a data classification (see Annex D).
- **Step 0b:** The business owner should create and maintain a whitelist of acceptable cloud services providers.
- **Step I**: The business owner forwards the request and data classification for a cloud service (or in general a new service) to the point of contact in the organization for IT-Services Deployment.
  - If the requested cloud service is on the corporate whitelist and matches data classification proceed to Step II.
  - If the requested cloud service is on the corporate whitelist but does not match data classification, the IT-Service department should contact the business owner and decide if a different cloud service from the whitelist can be used or if the selected could service should be re-evaluated for the desired protection level.
  - If the requested cloud service is on the corporate blacklist, the user should be informed of this and be directed to the whitelist.
  - If the requested cloud service is not on the corporate whitelist, the user should specify what type of problem needs to be solved by the cloud service. On that basis an alternative should be recommended to the user (maybe a cloud service from the whitelist).

- **Step II:** If the cloud service is already approved for the protection level of the data (see Annex D, data classification), access will be granted to the business owner.
- **Step III:** If the cloud service is new to the company, the request should be transferred to the IT and Legal Departments for approval. The user should define the demands/requirements for functionality and security:
  - What type of information is involved?
  - Data protection level of the information to process (public, internal, confidential, etc.)?
  - What should the cloud service do?
  - How do you want to use the service?
  - Will the information use or be used by other services?
  - Is it a B2B or B2C service?
  - Will the service be available to external users?
  - What service level (SLA) is required?

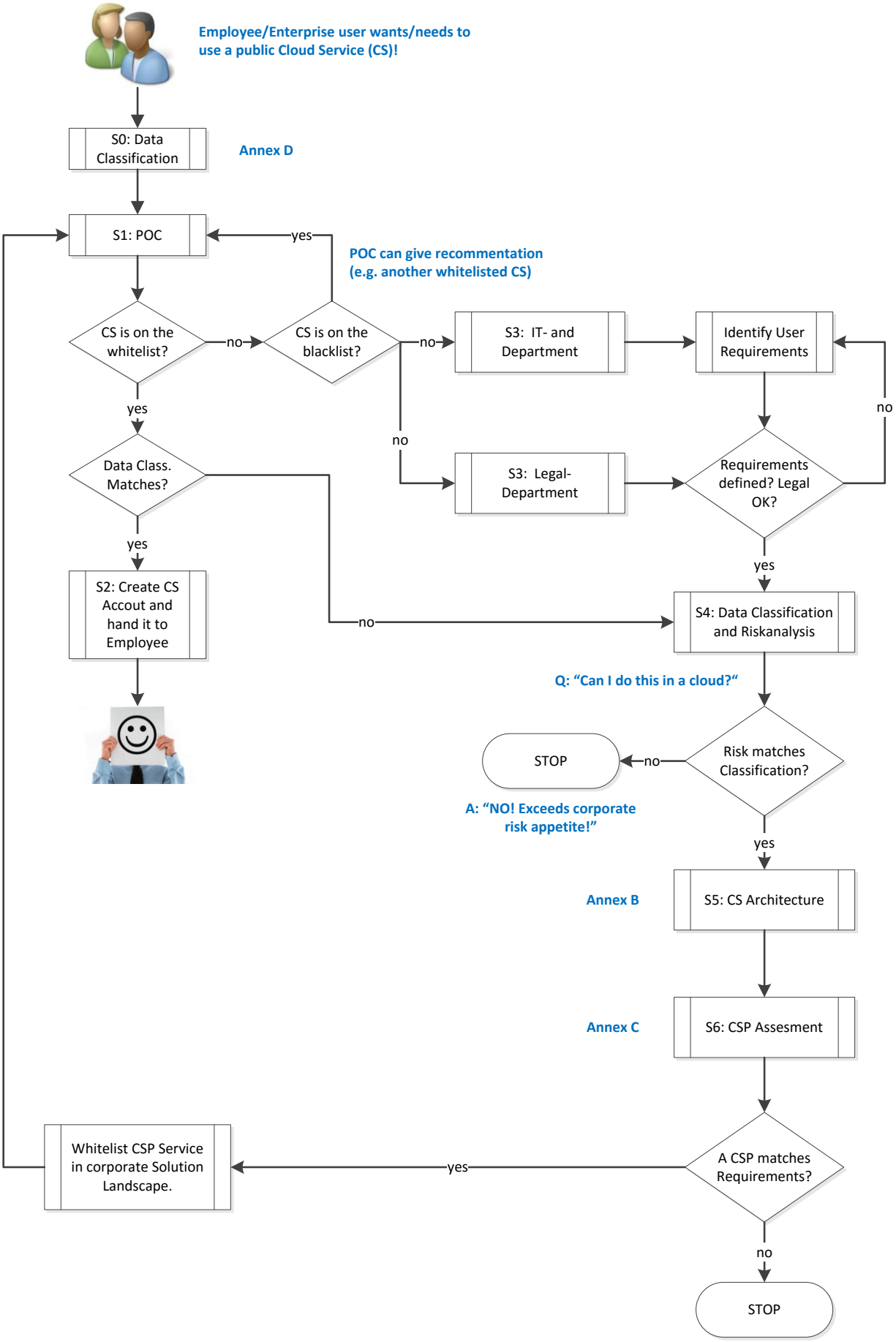

Figure A1: Workflow Example

- **Step IV:** The IT department performs a risk assessment based on the requirements from Step III.
  - What type of main threats regarding security and functionality can be identified?
  - What is the probability and impact of those threats?
  - What should be the cloud service's availability, integrity and confidentiality?
  - The risk assessment should be performed in cooperation with the service requestor to ensure that all current and future use cases, and the data they generate, are correctly covered.
    - The IT dept. is responsible for the technical aspects of the risk assessment
    - The requestor is responsible for the business aspects of the risk assessment

- **Step V:** The Cloud Solution Designer within the IT Department identifies the best Cloud Service Architecture to support the user demand. An on-premise solution should be preferred if the risk assessment from Step IV results in no applicable cloud service architecture that could provide the demanded level of security or functionality (for further details see Annex B).
- **Step VI:** The IT department performs a Cloud Service Provider Assessment based on Annex C.

Roles

Establishing a cloud service requires the intervention and interaction of different actors. The list below describes the main roles active in establishing a secured cloud service:

Business / Business Owner

The Business Owner demands a new service or functionality. This should usually be independent from a general cloud adoption discussion. The Business Owner also needs to classify the data (see Annex D).

Procurement

A Business Owner should not be able to purchase a service from a Cloud Service Provider directly. This should be centralized at the procurement department. If a business owner reaches out to the procurement department to buy a new service, they should forward the request to the Cloud Solution Designer.

Cloud Solution Designer

The technical expert choosing and "designing" the best applicable architecture as described in Annex B.

Legal Department

Legal usually covers all compliance and regulatory topics including special cases such as protection of journalist sources. The legal department should provide the regulatory boundaries for the Cloud Service Provider Assessment (see Annex C).

Data Privacy Officer

Sometimes the Data Privacy Officer is located within the legal department, depending on the company organization. Like legal, the DPO provides boundaries for personal identifiable information.

Chief Information Security Officer

The CISO provides all security requirements for the Cloud Solution Designer as well as risks

for the senior management related to the adoption of a cloud service.

Cloud Customer

The Cloud Customer describes the company or organizational unit that is planning to acquire and run cloud services from a Cloud Service Provider.

Cloud Service Provider

The service provider that offers cloud based services. Choosing the appropriate Cloud service Provider should be assessed as described in Annex C.

Annex B: Cloud Service Architecture

This annex describes an in-depth overview of a possible Cloud Service Architecture. The Cloud Service Architecture heavily relies on the chosen cloud service model and cloud deployment option.

B1. Cloud service models

- **Software-as-a-Service (SaaS)**. A SaaS model provides pre-installed software to customers who don't want to manage their applications and infrastructures.
- **Platform-as-a-Service (PaaS)**. A PaaS model usually consists of a hosted development environment, including application programming interfaces (APIs) and various operating platforms such as Windows or Linux (available in different configurations), and others. Organizations have more granular control over applications and data placed in the cloud, including controls for security and compliance.
- **Infrastructure-as-a-Service (IaaS)**. A IaaS model usually is an automated infrastructure provided by a Cloud Service Provider to Cloud Customers consisting of virtualized compute, storage and networking resource. Most Cloud Service Providers offer self-provision tools for the complete environment. This recommendation excludes potential physical server offerings of IaaS providers.
- **Container-as-a-Service (CaaS)**. CaaS is treated as a subset of IaaS in the context of this recommendation. It includes an additional layer (Container) above the operating system layer managed by the Cloud Customer, leaving more flexible control to the Cloud Customer.

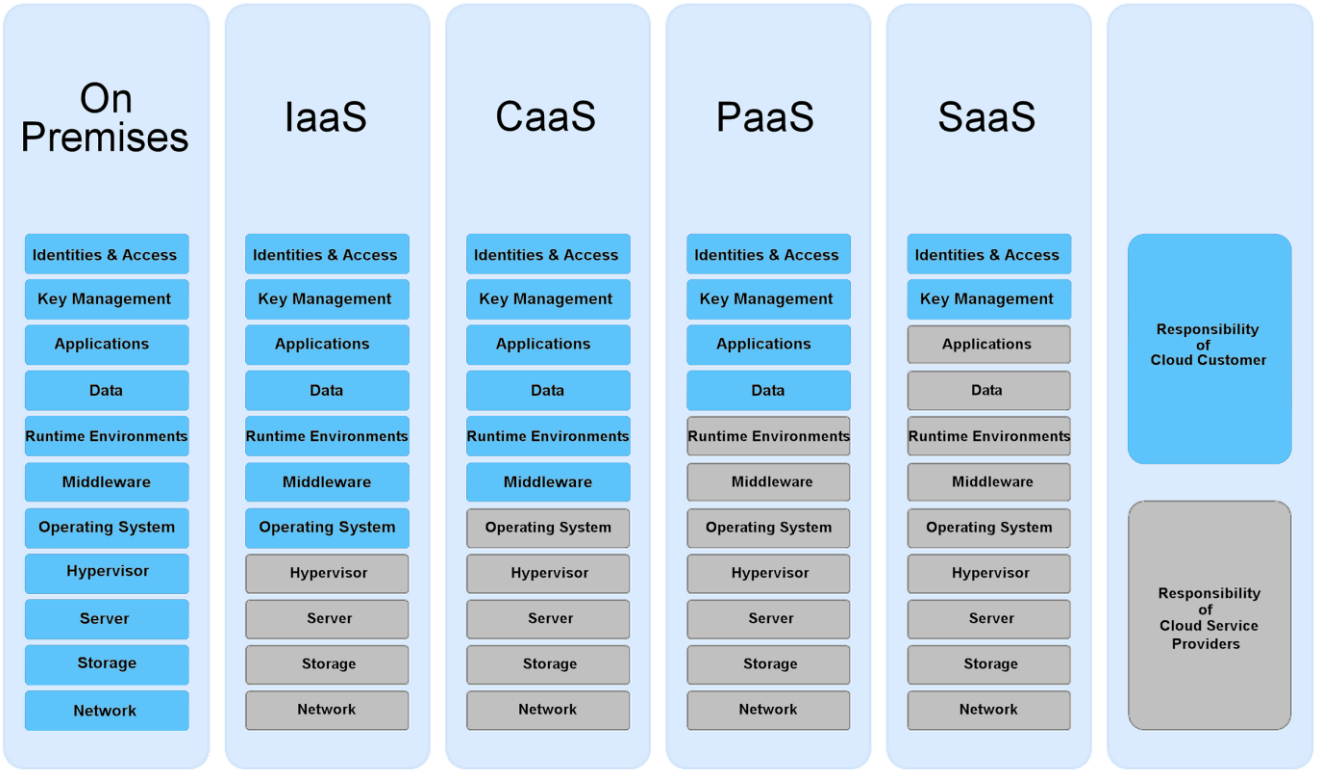

Figure B1: Cloud Responsibility Model.

B2. Cloud deployment options:

Any of these service models can then be deployed in a number of ways. The most common deployment options described by the Cloud Security Alliance (CSA) include:

- **Public:** Available to anyone via the Internet, associated with a Cloud Service Provider.
- **Private:** Internally developed clouds, provisioned internally or provisioned by a third party service provider, but only available to a single organization.
- **Community:** A cloud shared by multiple organizations with a common purpose or community.
- **Hybrid:** A combination of two or more of the three types mentioned, with possible data and/or application integration between them. An organization could, for example, use its internal cloud for specific business department uses (such as HR) and use Google to manage their email applications.

B3. Cloud Security Considerations

Each cloud model specifies the level of responsibility the Cloud Service Provider and/or the Cloud Customer need to fulfil.

As the cloud model specifies the degree of responsibility for each layer for the Cloud Service Provider and the Cloud Customer, the responsibility can be translated as trust of the Cloud Customer to the Cloud Service Provider. This level of trust increases from IaaS to SaaS and is described as a Simple Cloud Trust Model.

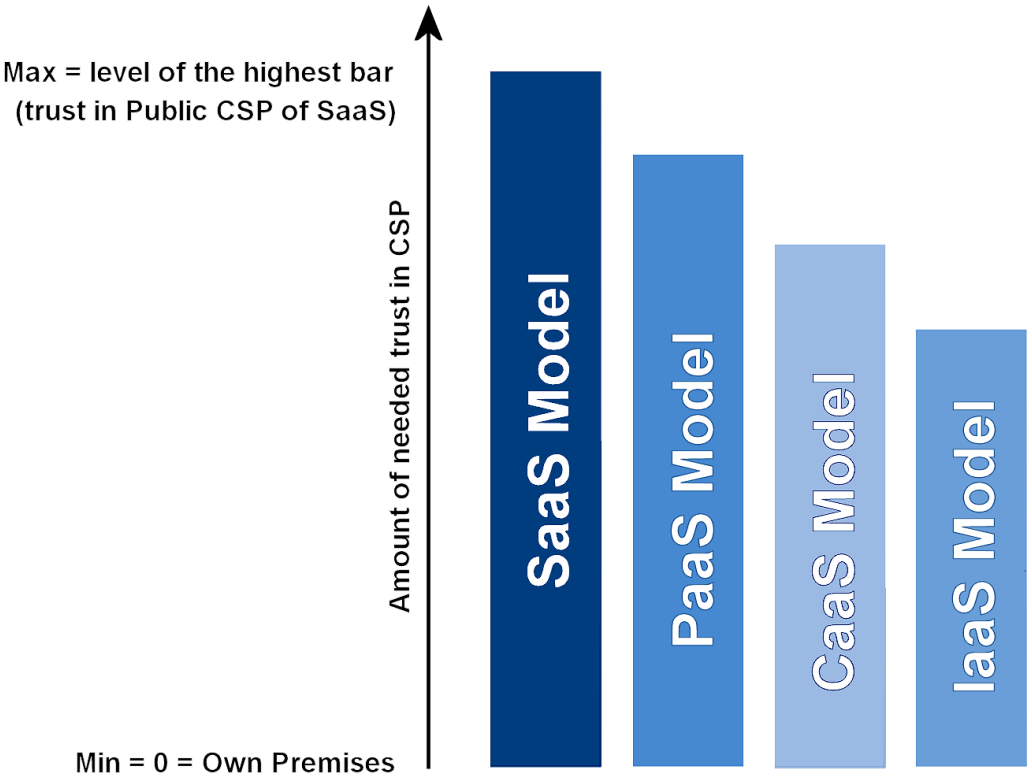

Figure B2: Simple Cloud Trust Model

In addition to that, the chosen delivery option (private or public) extends this Cloud Trust Model.

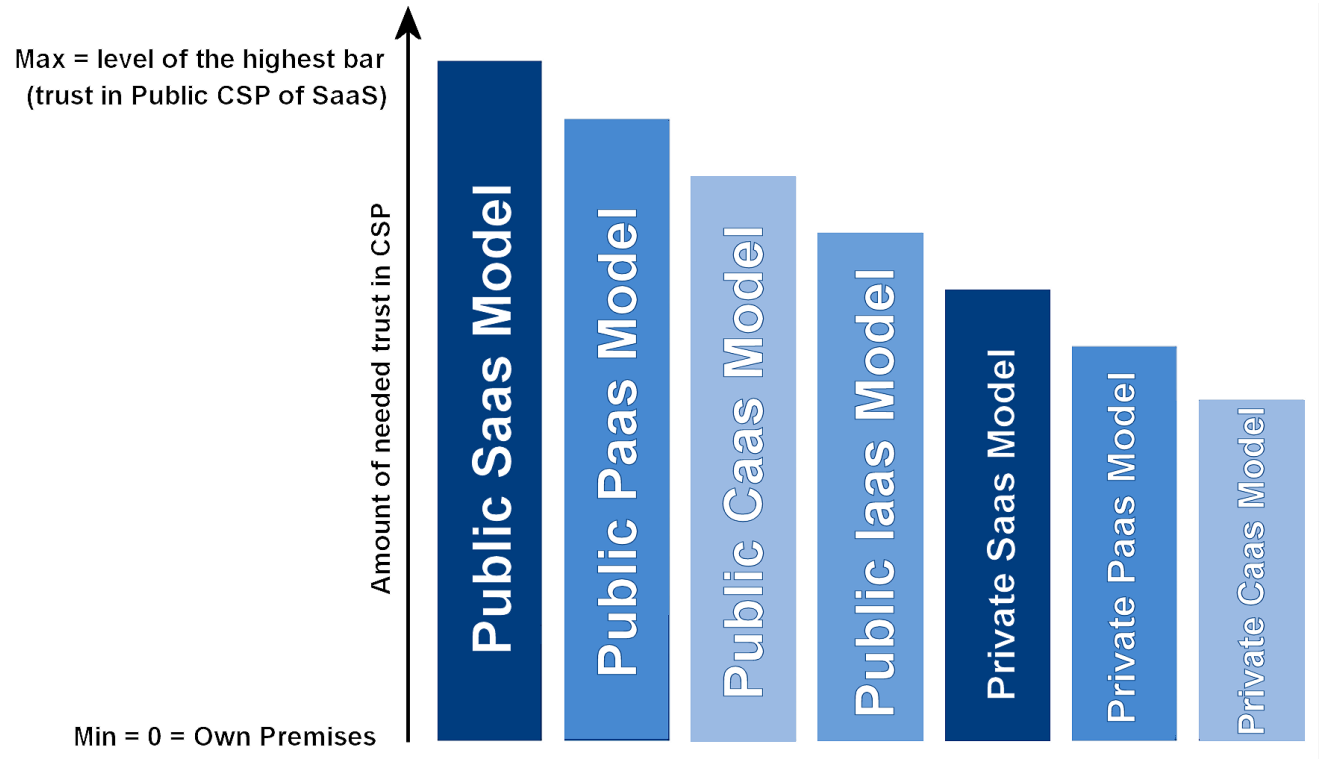

Figure B3: Extended Cloud Trust Model

The Simple and Extended Cloud Trust Model can be used for the Cloud Service Provider Assessment as described in Annex C.

If an appropriate Cloud Service Provider has been evaluated during the Cloud Service Provider Assessment (Annex C), the Cloud Customer can start deploying the needed solution. The architecture for the solution is depending on

1. **Confidentiality requirements:**
   Data that are processed need to fulfil potential data privacy and confidentiality needs,
2. **Integrity requirements:**
   Depending on the classification, integrity or non-repudiation features need to be deployed.
3. **Availability requirements:**
   Availability needs can be achieved by different architecture options (High Availability, Disaster Recovery, etc.).

The Availability, Integrity and Confidentiality requirements are determined during the data classification, as described in Annex D.

B4. Cloud Security Features

The Cloud Service Provider usually provides several security related features that need to be adopted by the solution to achieve the needed security requirements.

- *Identity and Access Management*
  Granting specific resources to specific users for a specific time. When moving to public cloud services multi factor authentication is strongly recommended.
- *Key Management Services*
  Management of licence keys for compliant activation of products and/or managing of cryptographic keys needed for encryption/decryption processes.

- *Administration Access*
  Access method for highest privileged users in order to manage systems or services.
- *Application management*
  Maintenance activities for keeping applications up to date and running.
- *Web Application Firewalling*
  Logical security gateway operating on the application level.
- *Secure APIs*
  Secure access and usage of APIs including access and authentication capabilities.
- *Logging*
  Logging capabilities throughout the different layers, preferably by dumping log events to a central Security Information Event Management system (SIEM).
- *IDS/IPS*
  Intrusion Detection and/or Protection capabilities usually operating on the networking layer.
- *DDOS Protection*
  Protection functionalities against Distributed Denial of Service attempts.
- *CDN Services*
  Content Delivery Networks provide distributed high availability and high performance access to content.
- *Middleware and Runtime Environment Management*
  Maintenance activities for keeping middleware and runtime environments up to date and running.

- *OS Management*
  Maintenance activities for keeping operating systems up to date and running.
- *Cloud Firewalling*
  Traditional Firewalling functionalities (up to UTM features) within the cloud network.
- *Cloud Network Access*
  Access options for Cloud Networks (limited, open, direct connections).
- *Cloud Virtual Networking*
  Virtual network layer within the cloud including separation considerations and load balancing functionalities.
- *Encryption on transit*
  Encryption for all data that are transferred (e.g. https, ftps ...).
- *Encryption at rest (on storage)*
  Hard disk or file system encryption.

Depending on the delivery model, providing and operating these Cloud Security Features are the responsibility of the Cloud Customer or the Cloud Service Provider.

Table: Security Functionality Responsibilities

		DELIVERY MODELS			
		IaaS	CaaS	PaaS	SaaS
SECURITY FEATURES	Identity and Access Management				
	Key Management Services				
	Administration Access				
	Application Management				
	Web Application Firewalling				
	Secure APIs				
	Secure Logging				
	IDS/IPS				
	DDOS Protection				
	CDN Services				
	Middleware and Runtime Environment Management				
	OS Management				
	Cloud Firewalling				
	Cloud Networking Access				
	Cloud Virtual Networking				
	Encryption on transit				
	Encryption at rest				

Customer Responsibility

Shared Responsibility

Cloud Service Provider Responsibility

B5. Examples on how to work with Cloud Security Features during the Cloud Service Design phase.

B5.1 Single System layout IaaS deployment

The Cloud Solution Designer needs to understand the confidentiality, integrity and availability requirements and based on the circumstances chose the best deployment option (IaaS, CaaS, PaaS, and SaaS). The following example shows a single instance and the different Cloud Security Features "surrounding" a single system.

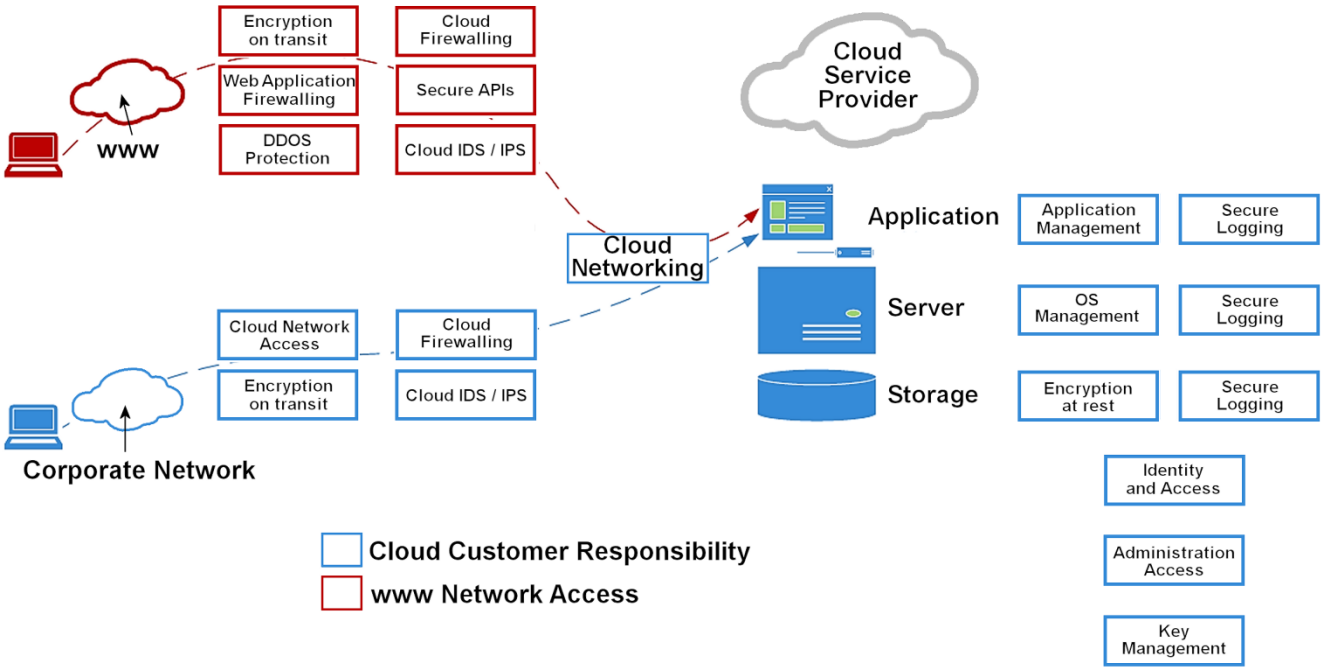

Figure B4: Single System layout SaaS deployment

Depending on the access to the application and its purpose, different Cloud Security Features may be deployed for the web access than for a more limited corporate access.

B5.2 Single System layout PaaS deployment

If the deployment options PaaS or SaaS is chosen, parts of the Cloud Security Features have to be provided by the Cloud Service Provider and therefore have to be included into the SLAs or purchased as an additional "option".

Some functionality will require a shared responsibility where, for example, the Cloud Service Provider might provide the infrastructure or needed application and the Cloud Customer handles the configuration (e.g. activation of https).

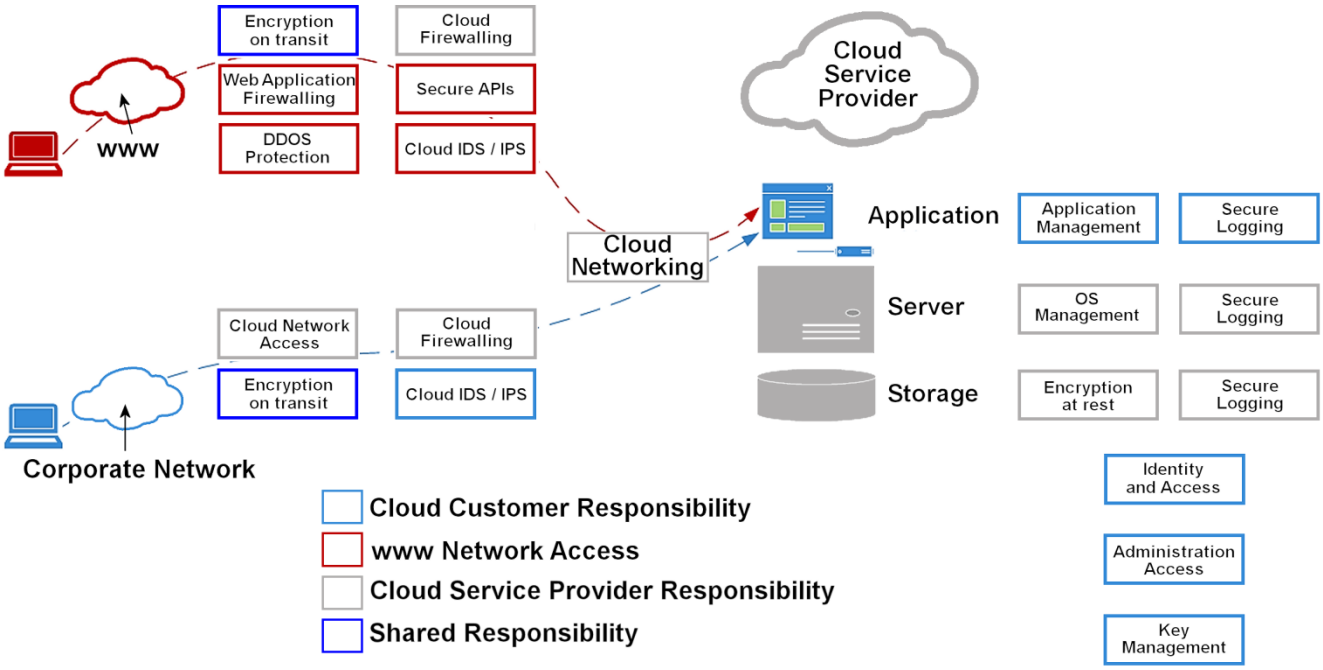

Figure B5: Example of Single System layout PaaS deployment.

B5.3 High Availability (HA) System layout IaaS deployment

If higher availability requirements need to be met, an additional instance needs to be considered and combined with the existing one, using the appropriate high availability (HA) architecture for clustering applications (e.g. on the application layer, on the DB layer or with data replication on the storage layer).

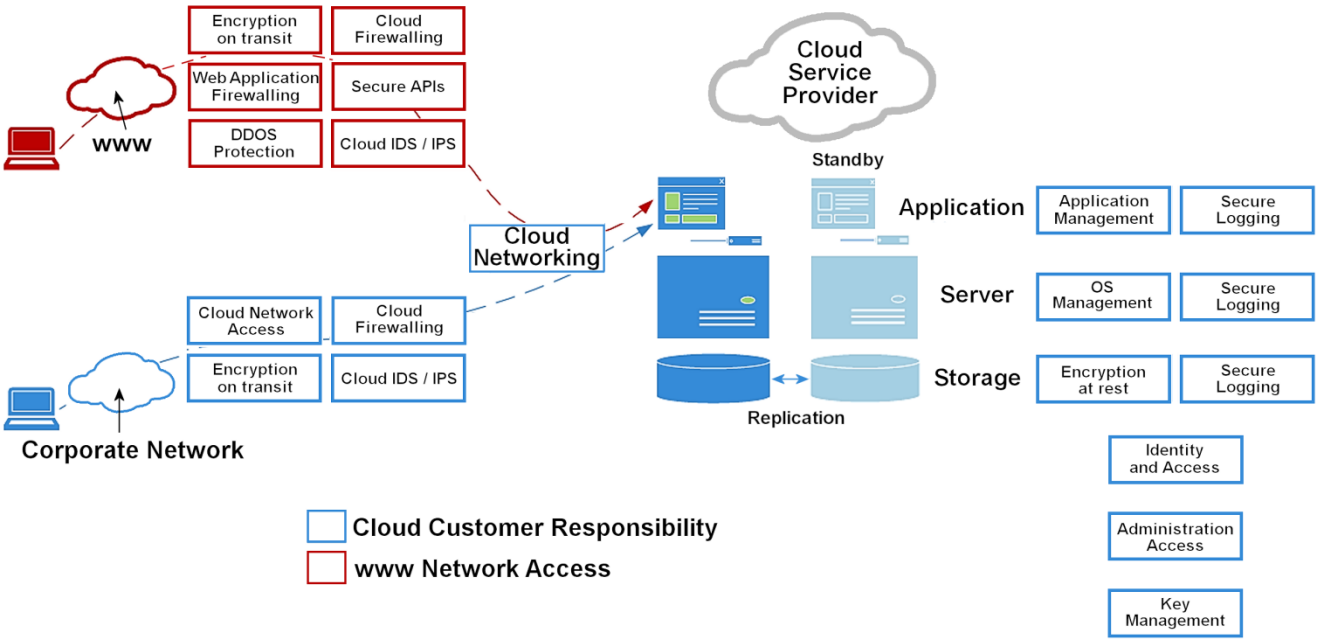

Figure B6: HA System layout IaaS deployment

For disaster recovery (DR), another cloud datacentre/region or on-premises instance may be considered. It is very important to understand the availability capabilities of a Cloud Service Provider. Past incidents have shown that many Cloud Customers neglect the possibility of a Cloud Service Provider region's outage. To achieve high availability, different Cloud Service Provider regions need to be included into the architecture options.

Annex C: Cloud Service Provider Assessment

The aim of this annex is to provide a consistent practice for assessing a Cloud Service Provider in the context of information security. When an organization considers using a certain cloud service, it needs to determine whether it is preferable over a competing offer or an internal solution. This not only requires a functional comparison between available cloud services and potential in-house solutions, it also means looking beyond the features provided to assess the companies behind the proposed cloud services.

Cloud Service Providers (CSPs) come in many different shapes and sizes, ranging from very large platforms to small niche players. This makes evaluating the security of those CSPs a difficult task. Also, by their very nature, cloud services limit your options for mitigating certain risks. As an example, many cloud services are available from anywhere through a web interface, increasing the attack surface as compared to internal solutions which may require a VPN.

It is beyond the scope of this annex to provide exhaustive questionnaires for the assessment of these CSPs. This annex summarizes the most important topics from some excellent work that has already been done on the subject, and provides useful references if further detail is required. Some references point to existing questionnaires, which will typically touch on the topics listed below. At the very least, the questions outlined in this annex should be answered, either by a CSP representative or a clear set of documents provided by the CSP.

C1. Certifications, standards, best practices

Does the CSP have any relevant information security certifications?

It might be interesting to avoid performing a full evaluation of CSPs if a provider holds certain certifications or it attests to following industry standards or best practices. Some examples of relevant security and/or operational frameworks include ISO-27001 or PCI-DSS. Another noteworthy initiative is the Security, Trust and Assurance Registry (STAR) maintained by the Cloud Security Alliance (CSA). The CSA STAR contains security assessments for many CSPs, either based on self-assessment or on third-party assessment.

Please note that further investigation on other topics in this annex should still be done, because security certificates do not always cover all the relevant topics.

C2. Legal and compliance

Is the organization (legally) allowed to let this data be processed by the CSP?

There are national and international laws that describe what organizations can and cannot do with certain kinds of data. In particular the EU General Data Protection Regulation is a key law to comply to for all service run in EU nor by EU organisations. The GDPR law provide a legal framework around (but not only) user data collection, storage and processing. It is important especially in the case of cloud based services to carefully verify and mandate the compliance to this regulation.

Most of the time, organizations have internal compliance rules as well. It is also important to consider the motivation of the CSP to offer the service. For instance, if the service is offered at a very low price or even for free, it is possible that the CSP's earnings model is to sell (meta)data to other parties.

Some subjects to consider:

- Applicable laws governing the use of this service or the data. Special data like "sources of journalists" need to be examined too.
- Applicable internal compliance rules governing the use of this service or the data.
- Terms and Conditions if ownership of the data is somehow transferred.
- Geographical regions where data is processed.
- Whether the data or metadata is used in any way by the CSP or any third party.

C3. Data security

How does the CSP guarantee the confidentiality and integrity of your data?

A CSP can only add value if it is going to process data in some way. It is important that the CSP has processes and systems in place to guarantee the confidentiality and integrity of the data. Because of privacy laws, special care should be taken when working with personally identifiable information (PII).

Some subjects to consider:

- The protection of the stored data at the CSP, both on a physical and logical level.
- The way data is protected while being transferred to and from the CSP or between its systems.
- The strength of the CSP's encryption, and how keys are managed.
- Who has access to the data?
- The data retention policy and the way data is securely deleted.
- How the different customers of the CSP in a multi-tenant system are isolated from each other.

C4. Availability

What measures are taken by the CSP to guarantee reliability and performance?

Downtime can potentially severely impact business processes, so the reliable availability of a (cloud) service is very important. Another important factor to consider is the availability of the data when an organization needs to transition from one CSP to another, or from the cloud to an internal solution.

Some subjects to consider:

- The applicable Service Level Agreements.
- Check if the CSP has implemented a business continuity plan.
- Protection against (D)DoS attacks.
- Check if the CSP provides easy and portable access to your data if you decide to stop using the service.
- The increased importance of internet access to be able to use the cloud service.

C5. Authentication and authorization

How are users, administrators and systems authenticated by the CSP?

Identity and Access management is crucial to securing information. This process ensures that everyone has appropriate access to resources across increasingly heterogeneous technology environments. Cloud services are a new kind of environment for most companies, so they should be integrated into corporate IAM to provide authentication and authorization mechanisms consistent with actual company policies.

Some subjects to consider:

- The available authentication and authorization mechanisms.
- Integration support with your existing IAM.
- The possibility of managing a mix of internal and external users.
- If granular control of different access levels exists.
- The authentication of API calls.
- The availability of audit logs.

C6. Organizational

Does the CSP have the organizational structure to keep our data secure?

A CSP can only protect the service and the data if the CSP's internal business processes support it.

Some subjects to consider:

- The transparency of the on-boarding process of new staff at the CSP.
- The available information about security incident handling.
- If the CSP uses any subcontractors to provide its service.

C7. Existing CSP assessment materials

As mentioned in the introduction, a lot of information on this subject is already available. Interesting publications include:

- **CSA**: https://cloudsecurityalliance.org
  - The Cloud Security Alliance is the leading organization dedicated to defining and raising awareness of best practices to help ensure a secure cloud computing environment. An excellent document is the "Security Guidance for Critical Areas of Focus in Cloud Computing" which aims to provide guidance and inspiration to support business needs while managing new risks. Another great resource is the CSA STAR Registry, which contains hundreds of security assessments of CSPs.
- **ENISA**: https://www.enisa.europa.eu/
  - The European Union Agency for Network and Information Security (ENISA) is a centre of expertise for cyber security in Europe. They have conducted a risks assessment on cloud computing business model and technologies. The result (a whitepaper called "Cloud Computing Risk Assessment") is an in-depth and independent analysis that outlines some of the information security benefits and key security risks of cloud computing.
- Another good resource for further documentation might be your national Cyber Security Centre or CSIRT.

Annex D: Data Classification

One key element of every risk assessment is data classification, meaning categorizing the processed data in their value to the organization. The systems processing the data as well as the resulting services provided by the systems inherit the classification from the data. A common practice is to differentiate the classification between “availability”-, “integrity”- and “confidentiality”-targets referred to as the AIC-triad. Additionally, “non-repudiation” can be seen as well as an optional protection target.

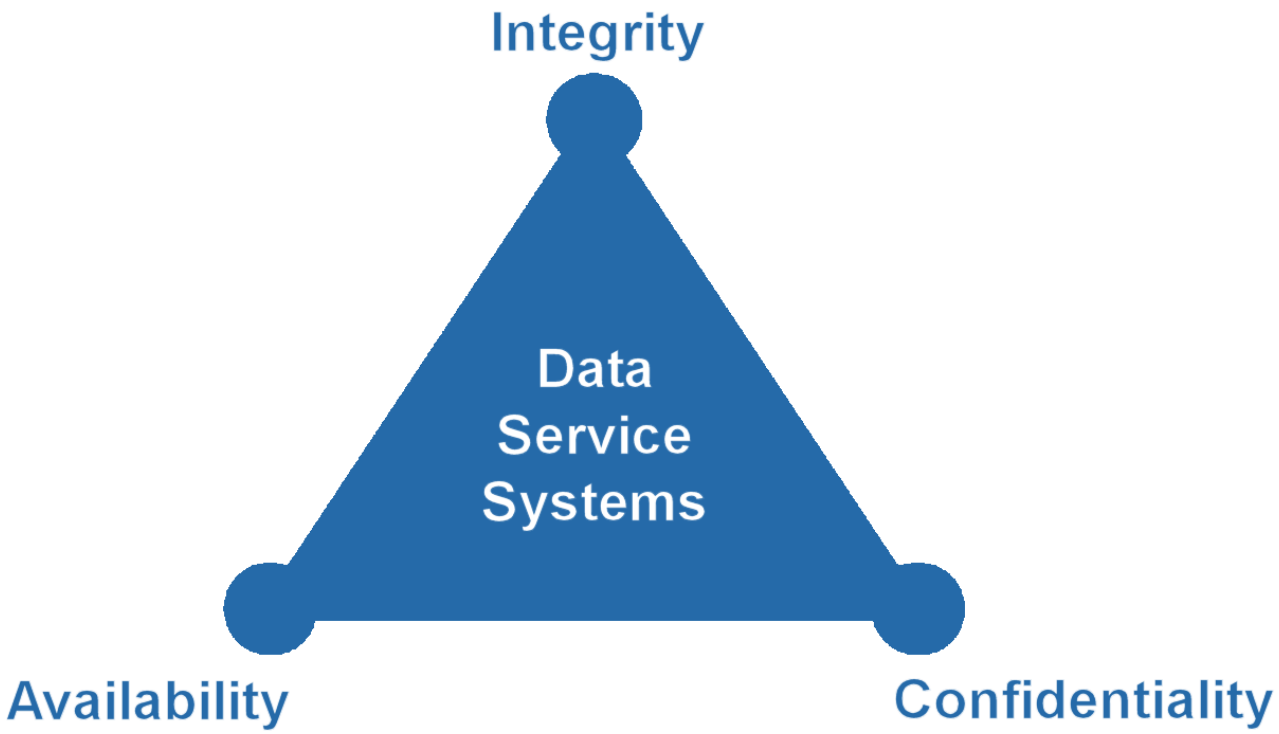

Figure D1: AIC triad

D1. Base rules for data classification

The creator or owner of information is always responsible for the classification (data owner). The requirements for

- Availability
- Integrity and
- Confidentiality

have to be defined by the Business Owner or the accountable individual person. The operating IT organization or Cloud Service Provider processes the data on behalf (data custodian).

For reducing the efforts of a complete data-classification, unclassified should be pre-classified if the data owner doesn’t decide otherwise. An internal default and external default classification scheme is highly recommended.

Usually the aggregated classification level (for data, systems and services) follows the highest classification even if a subset of information is already classified with a lower classification.

For processing and storing data on external systems like Cloud Service Providers, the external

systems need to be classified accordingly. Based on the classification more security controls may need to be applied for protection. Data may only be processed on systems that match the required classification requirements.

D2. Availability

The availability refers to the ability to successfully perform a requested function or information at any time within a specified time interval.

The higher the availability requirements for the business are, the higher the technological protection and availability requirements are (applications, systems, networks). The availability levels should be based on the potential damage and related to a risk management process.

The availability is usually defined in the following levels:

- Low (corresponds to a very low level of availability, no impact)
- Medium (corresponds to a medium level of availability, potential important impact)
- High (corresponds to a very high level of availability, potential catastrophic impact)

D3. Integrity

The integrity describes the "correctness" of information and the accurate functioning of systems.

The higher the integrity requirements for the business are, the higher the technological protection and integrity requirements are (applications, systems, networks). The integrity levels should be based on the potential damage and related to a risk management process.

The integrity is usually defined in the following levels:

- Low (corresponds to a low level of integrity, potential minor or no impact)
- Medium (corresponds to a medium level of integrity, potential important impact)
- High (corresponds to a high level of integrity, potential critical or catastrophic impact)

D4. Confidentiality

Confidentiality describes the character of an information to be accessible and available for a limited amount of recipients. The higher the confidentiality requirements for the business are, the higher the technological protection requirements are (applications, systems, networks).

Data privacy aspects have to be examined too as well as specific local regulations (e.g. protection of journalist sources).

Confidentiality is usually defined in the following levels:

- public (explicitly intended for the public)
- internal (freely available within the company)
- confidential (intended for a small target group)
- strictly confidential (intended for just a few people)

Bibliography

EBU	R144 – Cybersecurity Governance for Media Companies	https://tech.ebu.ch/publications/r144
EBU	R143 – Cybersecurity for media vendor systems, software & services	https://tech.ebu.ch/publications/r143
NIST	NIST Definition on Cloud Computing	http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf
Cloud Security Alliance	Cloud Controls Matrix	https://cloudsecurityalliance.org/group/cloud-controls-matrix/#_overview
Cloud Security Alliance	Star I Self Assessment	https://cloudsecurityalliance.org/star/#_overview
Amazon	AWS Security Best Practices	https://aws.amazon.com/de/whitepapers/aws-security-best-practices/
Microsoft	Azure Security Best Practices	https://docs.microsoft.com/en-us/azure/security/security-best-practices-and-patterns
Google	Google Cloud Platform Best Practices for Enterprises	https://cloud.google.com/docs/enterprise/best-practices-for-enterprise-organizations
enisa	Cloud Computing: Benefits, risks and recommendations for information security	https://resilience.enisa.europa.eu/cloud-security-and-resilience/publications/cloud-computing-benefits-risks-and-recommendations-for-information-security/view
enisa	Critical Cloud Computing	https://resilience.enisa.europa.eu/cloud-security-and-resilience/publications/critical-cloud-computing/view
UK NCSC	Cloud Security Collection	https://www.ncsc.gov.uk/guidance/cloud-security-collection
French ANSSI	Prestataires de service d'informatique en nuage (SecNumCloud)	https://www.ssi.gouv.fr/administration/qualifications/prestataires-de-services-de-confiance-qualifies/prestataires-de-service-dinformatique-en-nuage-secnumcloud/
German BSI	German BSI Cloud Computing Catalogue	https://www.bsi.bund.de/EN/Topics/CloudComputing/CloudComputing_node.html;jsessionid=7D7F696F4635F963469E8B57F2CE35CA.2_cid351
ISO	ISO/IEC 27018:2014 Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors	https://www.iso.org/standard/61498.html
ISO	ISO/IEC 27017:2015 Security techniques -- Code of practice for information security controls based on ISO/IEC 27002 for cloud services	https://www.iso.org/standard/43757.html
EU	EU General Data Protection Regulation	http://www.eugdpr.org