# Cloud Assurance

Cloud assurance extends beyond just the quality of a cloud service. More and more companies are considering leveraging cloud services for business processes. These companies expect **assurances from their cloud providers of their security and reliability**. The "Information Assurance Framework" from the „European Network and Information Security Agency" (ENISA) defines a **set of assurance criteria** (PDF-Download). ENISA recommends that companies get potential cloud providers to provide answers to the questions in order to be able assess their reliability.

The question catalog is split into ten main categories. In the following sections Fabasoft provides concrete answers to ENISA's questions for the Fabasoft Cloud Platform.

## Personnel Security

### ENISA criteria:

This is about security measures for the cloud provider's personnel. What policies and procedures do you have in place when hiring your IT administrators or others with system access? Are there checks concerning identity, CV and criminal records before employing new personnel? What security education program do you run for all staff? Is there a process of continuous evaluation?

### Fabasoft response:

Fabasoft makes sure that all employees are made aware of the topic of information security. Upon joining the company all employees must submit a criminal records check and sign a data protection declaration and an information security agreement. Regular training on the topic of information security takes place in the **Fabasoft Academy**. Furthermore, Fabasoft fulfills all the requirements for personnel security under the **ISO 27001 certification** and **ISAE 3402 Type 2 audit** conducted by PricewaterhouseCoopers. This particularly concerns **full traceability and transparency** in the cloud data centers: Each activity must be planned, announced and approved before execution. The execution must be documented and traceable.

## Supply chain assurance

### ENISA criteria:

These criteria apply where the cloud provider subcontracts some operations that are key to the security of the operation to third parties. This mainly affects cloud providers who outsource the underling platform (Infrastructure as a Service) to a third party provider, for example operating their cloud services on Amazon or German Telecom's platforms. In this case the cloud provider must detail the procedures used to assure third parties accessing your infrastructure (physical

and/or logical). Are the service levels offered to the cloud provider's customers also guaranteed by the third parties?

### Fabasoft response:

Fabasoft provides its cloud services using exclusively its own resources. Fabasoft operates its own cloud hardware in high-performance data centers and merely rents space including cooling and fail-safe power and internet connections. These data center providers are:

Cloud location Germany: noris network AG

Cloud location Austria: T-Systems Austria GesmbH

Cloud location Switzerland: Deltalis SA

**The complete source code** for the cloud services, including the operating and database systems (Enterprise Linux and PostreSQL), **is on Fabasoft's premises**.

## Operational security

### ENISA criteria:

In addition to the guarantee of service levels, a company should still ensure that the cloud provider employs appropriate controls to mitigate unauthorized disclosure of customer data. This needs to be clarified in the areas of software assurance, patch management, network architecture controls, host architecture, resource provisioning, PaaS application security and SaaS application security.

**Software assurance:** How does the cloud provider protect the integrity of the operating system and applications software used? What standards are adhered to? Are environments in place to reduce risks, e.g. development, test and operation environments, and these environments kept separate from each other? What controls offer protection against dangerous code? What guidelines and procedures exist for backups?

**Patch management:** What patch management procedure is followed? Does the cloud provider ensure that the patch management process covers all layers of the cloud delivery technologies – i.e., network, server operating systems, virtualization software, applications and security subsystems?

**Network architecture controls:** What levels of isolation are used (for virtual machines, physical machines, network, storage etc.)? Does the architecture support continued operation from the cloud when the company is separated from the service provider and vice versa (e.g., is there a critical dependency on the customer LDAP system)?

**Host architecture:** Is the host firewall run with only the minimum ports necessary to support the services within the virtual instance?

**PaaS application security:** Can a Platform as a Service (PaaS) provider guarantee the security of its platform? What assurance can the PaaS provider give that access to your data is restricted to

your enterprise users and to the applications you own? Does the PaaS provider ensure that the platform is protected against vulnerabilities through applications?

**SaaS application security:** The SaaS model dictates that the provider manages the entire suite of applications delivered to end-users. Therefore SaaS providers are mainly responsible for securing these applications. What administration controls are provided? Can these be used to assign read and write privileges to other users? Are there detailed access rights controls and can these be adapted to a company's own organisational guidelines?

**Resource provisioning:** How much can you scale up? Does the provider offer guarantees on maximum available resources within a minimum period? What processes are in place for handling large-scale trends in resource usage (e.g. seasonal effects)?

### Fabasoft response:

Fabasoft strictly separates its development, test and productive systems. Software development takes place using the agile project management methodology **SCRUM**. The cloud services are updated monthly. The cloud services update is executed with **zero known defects**. This means that at the time of update, all defects found and captured by Fabasoft have been fixed. Each software build has to undergo extensive automatic tests in a **continuous integration environment** so that potential defects can be discovered as early as possible. Each cloud user can give direct feedback to defects or new cloud features via the support button in the cloud application. This flows directly into the agile software development, is prioritized and quickly addressed during the monthly cloud updates (**user experience management**).

## Identity and access management

### ENISA criteria:

A company should clarify a cloud provider's identity and access management systems: Authorization, Identity provision, management of personal data, key management, encryption, authentication, credential compromise or theft, identity and access management systems offered to the cloud customer.

**Authorization:** Do any accounts have system-wide privileges for the entire cloud system and, if so, for what operations (read/write/delete)? How are the accounts with the highest level of privilege authenticated and managed?

**Identity provision:** What checks are made on the identity of user accounts at registration? Are any standards followed?

**Management of personal data:** What data storage and protection controls apply to the user directory and access to it? Is user directory data exportable in an interoperable format?

**Encryption:** Where is encryption used (data in transit, data at rest, data in processor or memory)? Are usernames and passwords encrypted? Is there a well-defined policy for what should be encrypted and what should not be encrypted?

**Authentication:** What forms of authentication are used for operations requiring high assurance?

**Credential compromise or theft:** Do you provide anomaly detection (the ability to spot unusual and potentially malicious IP traffic and user or support team behavior)?

**Identity and access management:** This applies to the identity and access management systems which are offered by the cloud provider for use and control by the cloud customer. Is the cloud provider interoperable with third party identity providers? Is there the ability to incorporate single sign-on? Does the client credential system allow for the separation of roles and responsibilities and for multiple domains (or a single key for multiple domains, roles and responsibilities)? How does the cloud provider identify itself to the customer (i.e. is there mutual authentication)?

### Fabasoft response:

Every single communication between user devices and Fabasoft cloud services is protected via SSL encryption according to the RSA procedure (**HTTPS standard**). In the Fabasoft cloud data centers, data encryption takes place via self encrypting discs. At application level Fabasoft cloud services protect customer data from unauthorized access through the concept of team rooms. A team room is a protected area in the cloud to which only explicitly authorized (access rights: read/change/administration) business contacts who have been invited to the collaboration and who have securely authenticated themselves have access. A security level can be set per team room so that access is limited to people with higher authentication characteristics. Alongside authentication with username and password Fabasoft cloud services support **two factor authentication** (Mobile PIN), single sign-on via client certificates (X.509 standard, also for mobile devices) and login with a digital identity (Austria: mobile signature; Germany: new ID card; Switzerland: SuisseID). The authentication takes place via a Fabasoft IDP service which implements the standards SAML and OAUTH.

Fabasoft supports the modeling of companies with their organizational structure in the cloud (**cloud organizations**). Access rights in team rooms can therefore also be assigned to groups and organizational units as well as to individual users. The management of organization members and the definition of security characteristics can therefore be conducted centrally in the cloud.

## Asset management

### ENISA criteria:

It is important to ensure the provider maintains a current list of hardware and software (applications) assets under the cloud providers control. This enables checks that all systems have appropriate controls employed, and that systems cannot be used as a backdoor into the infrastructure. Is there a list of assets that the customer has used over a specific period of time? Does the provider have an automated means to inventory all assets, which facilitates their appropriate management?

Fabasoft response:

Fabasoft is **ISO 20000 certified** and therefore fulfills all requirements for this standard for the automatic management of hardware and software inventory.

## Portability of data and services

ENISA criteria:

This set of questions should be considered in order to understand the risks related to vendor lock-in. Are there documented procedures and APIs for exporting data from the cloud? Does the vendor provide interoperable export formats for all data stored within the cloud? are the API interfaces used standardized?

Fabasoft response:

Fabasoft cloud services support the **standards CMIS** (Content Management Interoperability Standard), **WebDAV** and **CalDAV** for the import and export of cloud data. This enables, for example, a Fabasoft cloud service to be set up as a **network directory** in Microsoft Windows or in Apple Macintosh Finder and for regular delta data matching out of or into the cloud to be executed via backup tools. Import and export of data in **XML format** is also possible.

## Business continuity management

ENISA criteria:

A cloud provider must plausibly present its continuity procedures in the event of disruption. Does the provider maintain a documented method that details the impact of a disruption? What are the RPO (recovery point objective) and RTO (recovery time objective) for services? What dependencies on suppliers and outsource partners relevant to the restoration process exist? Can the effects of a disruptive event be kept to an acceptable level (accident management)? Does the provider have a formal process for locating, identifying, analyzing and addressing incidents? Is this process tested and prepared so that an actual incident can be effectively overcome? How are incidents documented and evidence secured?

Fabasoft response:

Fabasoft fulfills the requirements for the continuity of cloud operation in case of disruption in accordance with **ISO 20000** certification and **ISAE 3402 Type 2** via PricewaterhouseCoopers audit demands.

# Physical security

## ENISA criteria:

Physical security is particularly important because many cloud providers outsource the control over their IT infrastructure. What assurances can the cloud provider provide to the customer regarding the physical security of the location? Who, other than authorized IT personnel, has unescorted (physical) access to IT infrastructure (e.g. cleaners)? How often are access rights reviewed? Are personnel who have access to secure areas monitored (including third parties)? Does the personnel use portable equipment (e.g. laptops, smart phones) which can give access to the data center?

## Fabasoft response:

All data centers are equipped with alarms which immediately alert the police in cases of attempted unauthorized entry. The data centers are also equipped with video surveillance and highly sensitive early fire detection and preventive fire protection. Naturally only authorized staff has access to the data centers.

# Environmental security measures

## ENISA criteria:

What procedures or policies are in place to ensure that environmental issues do not cause an interruption to service? What methods are used to prevent damage from a fire, flood, earthquake, etc?

## Fabasoft response:

The software in question operates in a total of **three data centers per Fabasoft Cloud location**. The active data centers (data center 1 and data center 2) are located at two different sites. The backup data center is located at the same site as data center 1.

The sites of the active data centers per Fabasoft Cloud location are **at least 2 km apart**. Both centers are equipped with redundant air conditioning and network infrastructure.

In case of power failure, all data centers can supply power to the components for up to 15 minutes. At least one data center per Fabasoft Cloud location can maintain the power supply to the components for longer periods of power failure via a UPS (**Uninterruptible Power Supply**) with a connected emergency diesel power generator.

The backup data center operates a backup infrastructure to secure all data. The backup data center is equipped with its own access rules, redundant air conditioning and network infrastructure as well as emergency power supply.

The data centers are also equipped with highly sensitive early fire detection and preventive fire protection.

## Legal requirements

### ENISA criteria:

Customers and potential customers of cloud provider services should have regard to their respective national and supra-national obligations for compliance with regulatory frameworks and ensure that any such obligations are appropriately complied with. In what country is the cloud provider located? Is the cloud provider's infrastructure located in the same country or in different countries? Where will the data be physically located? What happens to the data sent to the cloud provider upon termination of the contract?

### Fabasoft response:

The Fabasoft cloud data centers are located in Germany, Austria and Switzerland and therefore subject to **European data protection and data security laws**. With the new unique concept of cloud locations, Fabasoft offers its customers the freedom of choice and assurance of knowing where their cloud data is stored. This ensures that you always know where your data is.