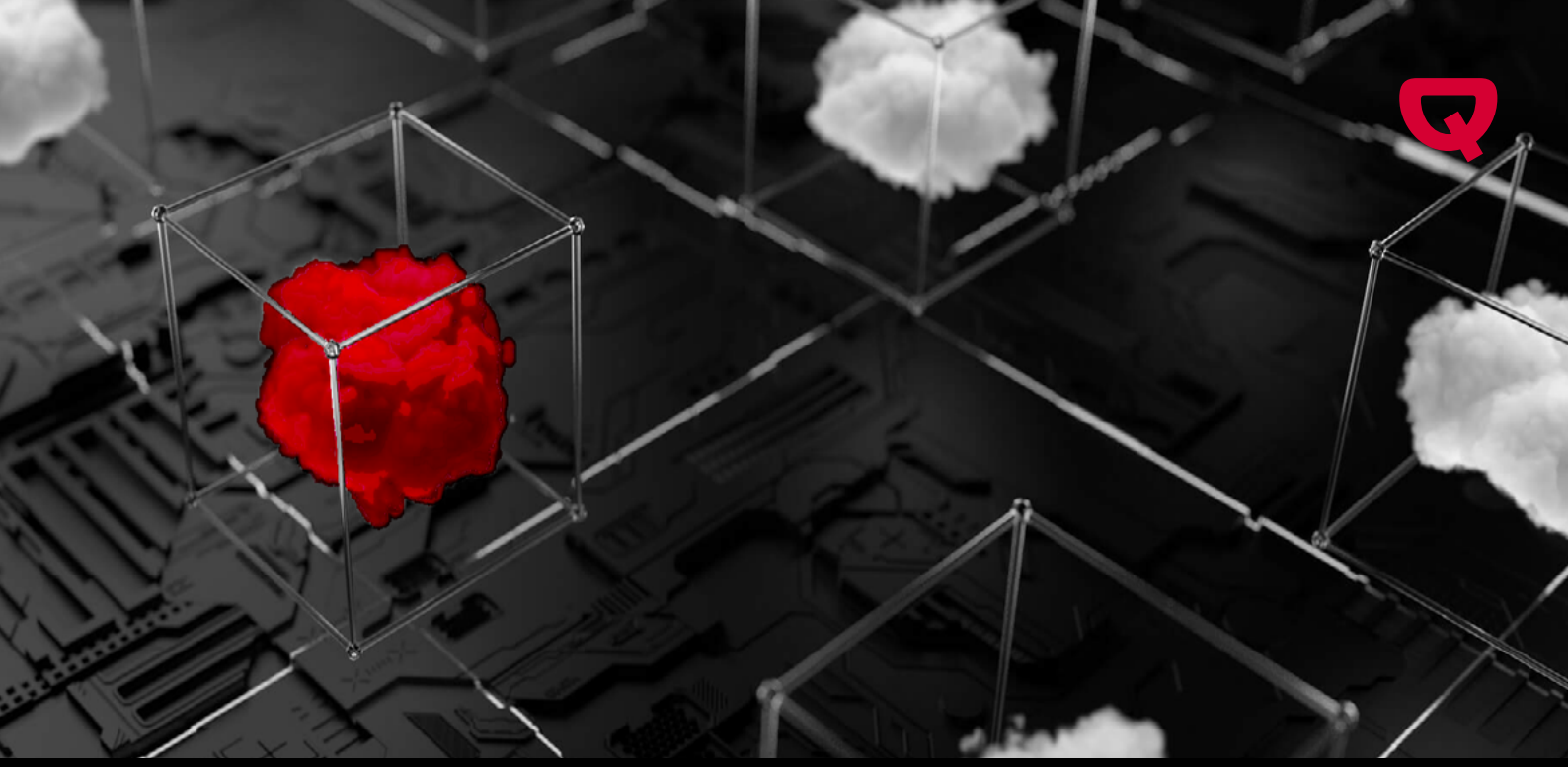

IT SECURITY REQUIREMENTS WHEN PURCHASING A SAAS SOLUTION

CLASSIFICATION

Ensure that your organization has classified the system and the Data as SaaS the solution must handle. Does the SaaS solution need to be able to handle different regulatory requirements? The classification of the data and any regulatory requirements shall govern the level of security. Does the supplier itself meet any of the regulatory requirements?

#GDPR, #PCI-DSS, #HIPAA/HITECH, #NIST, #CIS, #SOX, #SOC 2 Type II, ISO 27000

SDLC

Verify that the vendor has a defined secure software development cycle (SDLC). This must include secure development methodologies, vulnerability analyses, threat modeling and penetration tests by independent parties. To ensure vulnerabilities can be detected in each development phase and resolved before production. OWASP ASVS can be used to help create a requirements statement for web applications.

Has the supplier had security flaws in the past?
How to deal with security flaws?

INSTALLATION

The provider delivers a service that ensures data is secure, both in transactions as well as in savings. Ensure that data is segregated and that the infrastructure is hardened.

Are there multiple organizations in the same installation?
Dedicated or shared infrastructure?
Is data encrypted in the internal network?

BACKUP

Generating backups is an important part of ensuring business continuity. When an attack occurs and data is destroyed or deleted, a backup allows to quickly restore the system.

How often are backups created?
Do you need to configure this yourself?

SECURITY CHECKS

Security controls for SaaS applications are intended to be used to identify, avoid or reduce security risks. Ensure that your SaaS provider implements:

- Data encryption and tokenization:
  - Is PII data saved?
  - Do administrators have access to data in plain text?
  - End-to-end encryption (E2EE)
- Advanced virus prevention
- Data loss prevention
- Identity and access management:
  - Password Policy
  - Two factor authentication support
  - Access control Implementation
  - Privileged account Management
- Logging och monitoring:
  - Ensure that the provider logs and continuously monitors logs for suspicious behavior and attacks.

SECURITY PERSONNEL

Does the supplier have dedicated security personnel?

SUPPORT & SLA

Verify the provider's SLA for the service and ensure management of support is done within reasonable time.

SECURITY INCIDENTS

Is there a defined security incident plan?

QESTIT

qestit.com