enisa
European Network
and Information
Security Agency

Survey on Security Parameters in Cloud SLA's Among Public Sector and EU Institutions

Top-Level Analysis and Summary of Results

November 2011

About ENISA

The European Network and Information Security Agency (ENISA) is an agency of the European Union. It was established in 2004 to support the European Union and its Member States in network and information security. The Agency acts as a centre of expertise, giving advice and recommendations, and promoting good practices. The Agency also has a key role in facilitating contacts and the sharing of ideas between the European Institutions, the Member States, industry and the academic world.

Contact details:

For contacting ENISA or for general enquiries on xxxxx, please use the following details:

Hogben Giles, Expert hogben.giles@enisa.europa.eu

Internet: http://www.enisa.europa.eu/

Legal notice

Notice must be taken that this publication represents the views and interpretations of the authors and editors, unless stated otherwise. This publication should not be construed to be an action of ENISA or the ENISA bodies unless adopted pursuant to the ENISA Regulation (EC) No 460/2004 as lastly amended by Regulation (EU) No 580/2011. This publication does not necessarily represent state-of the-art and ENISA may update it from time to time.

Third-party sources are quoted as appropriate. ENISA is not responsible for the content of the external sources including external websites referenced in this publication.

This publication is intended for educational and information purposes only. Neither ENISA nor any person acting on its behalf is responsible for the use that might be made of the information contained in this publication.

Executive summary

Scope

This survey maps the **security aspects of service level agreements or similar contract arrangements** across governmental and other public sector organizations including EU institutions in the European Union.

Types of services covered

Cloud services as defined in ENISA's cloud security risk assessment (SaaS, PaaS and IaaS)

More traditional types of outsourced IT services, such as data-centre and hosting services (for website hosting, desktop virtualization, and so on), outsourcing services and network and communication services.

Target Group

IT professionals and decision makers in public sector organisations, who have been involved in procuring cloud services and or more traditional types of outsourced IT services

Survey Characteristics

Top-level summary

Total no of responses = 142

- 117 fully completed
- 25 valid dropouts

Follow-up

- 70 agreed to be approached for further collaboration on best practices

Cloud

- 9 pure cloud related contracts

Type of organization

- EU-level
- Central Government
- Municipal

15 EU countries involved

- Czech Republic
- Denmark

- Finland
- France
- Germany
- Hungary
- Ireland
- Italy
- Norway
- Poland
- Romania
- Slovakia
- Spain
- Sweden
- UK

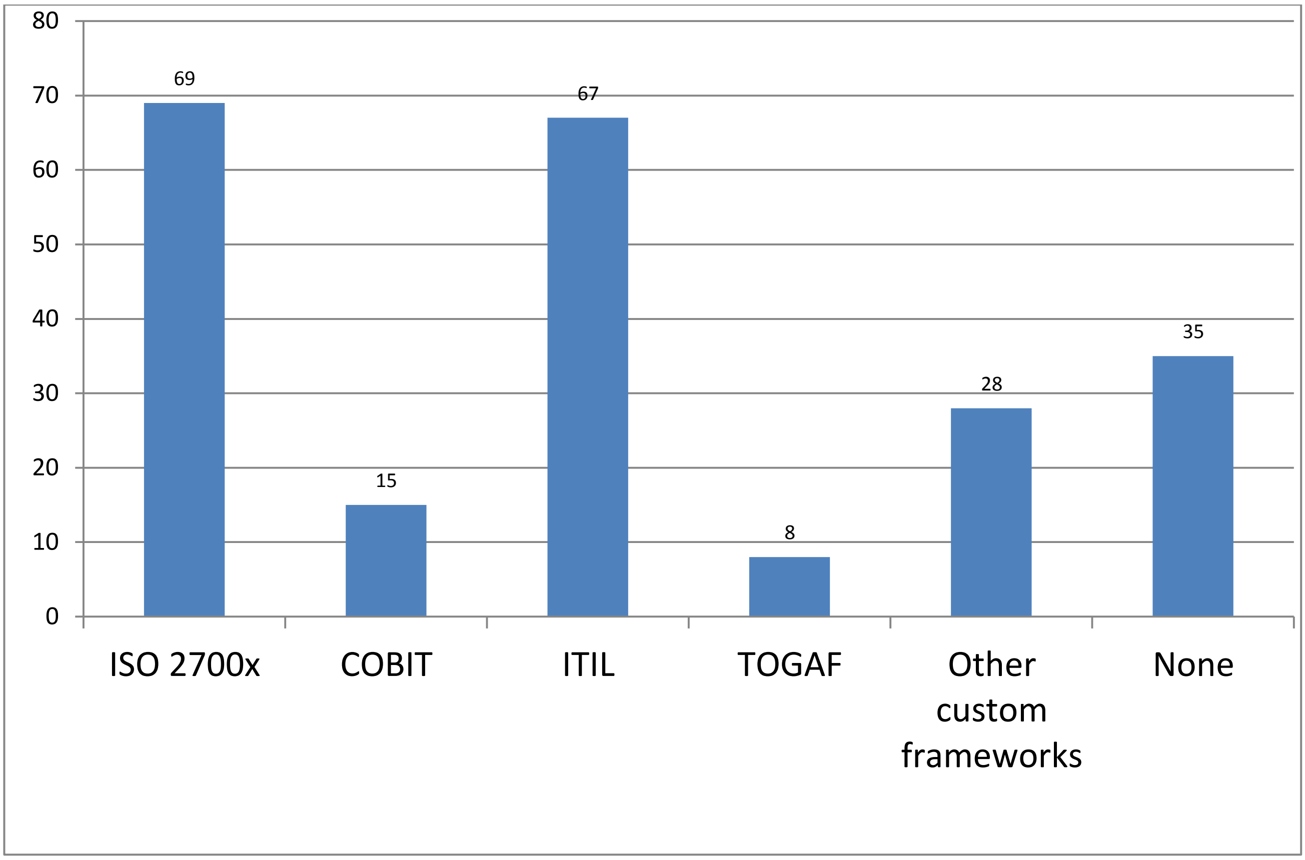
Contracts/SLAs

- Most of contracts are signed for 3 and more years and cover mostly providing internet connectivity and hosting services. Just 64% of the contracts include some kind of SLA.
- Contracts are usually drafted and reviewed by IT departments, but IT management is also often involved. Security specialists influence 63% of the contracts.
- Most of SLAs define penalties for breaching the SLA. Mostly the penalty is expressed as some percentage of the service fee. More detail can be seen in the pie on the right.

Security

- ITIL and ISO2700x are the most adopted standards among governmental institutions.
- More than 20% of the organizations do not use any governance frameworks or security standard.
- The adoption of various security standards and governance frameworks is visualized in the following chart.
- Security is a big concern of 77% of governmental organizations.

Adoption of various security standards and governance frameworks



Security parameters in SLA

- Availability is the most important parameter mentioned in SLAs. For governmental organizations, a service is available when it can be reached by all clients and most frequently, it is calculated for one month or one year. When the service becomes unavailable, in 78% of the cases the provider is obligated to report the service outage to the customer.
- 75% of contracts have defined maximum recovery time, while at least 50% of all contracts define penalties for breaching the recovery time and at least 25% of the contracts do not define any penalties.
- Besides availability, SLAs commonly cover redundancy, backups and access control. Other parameters are less frequent.

Measurement of security parameters

- As much as 15% of the contracts do not include availability measurements while the rest does. 50% of the contracts define that availability is measured regularly and 27% perform irregular measurements. In 63% of cases, availability is measured by the customer.

- More than 57% of customers have performed penetration tests, but only 16% of them run penetration tests regularly. The interesting fact is that these test are predominantly carried out by independent organizations.

- Backup and failover systems have been tested by 65% of customers and the tests are mostly irregular. In 56% of cases, these tests are carried out by the customer.

- There is one parameter of the service that has not been too much tested – data portability. Almost 40% of contracts do not include any tests if the customer's data can be taken to another service provider. Usually it is the customer who tests the portability.

- Load testing has been performed by 59% of customers and is usually irregular. From 51%, load testing is carried out by the customer while in 41% of the cases, it is the service provider who takes care of these tests.

- Only 39% of the organizations run unit tests and these test are performed on an irregular basis.

Reporting

- Providers usually report on availability, penetration test results, failover and backup systems tests and also on various unit tests.

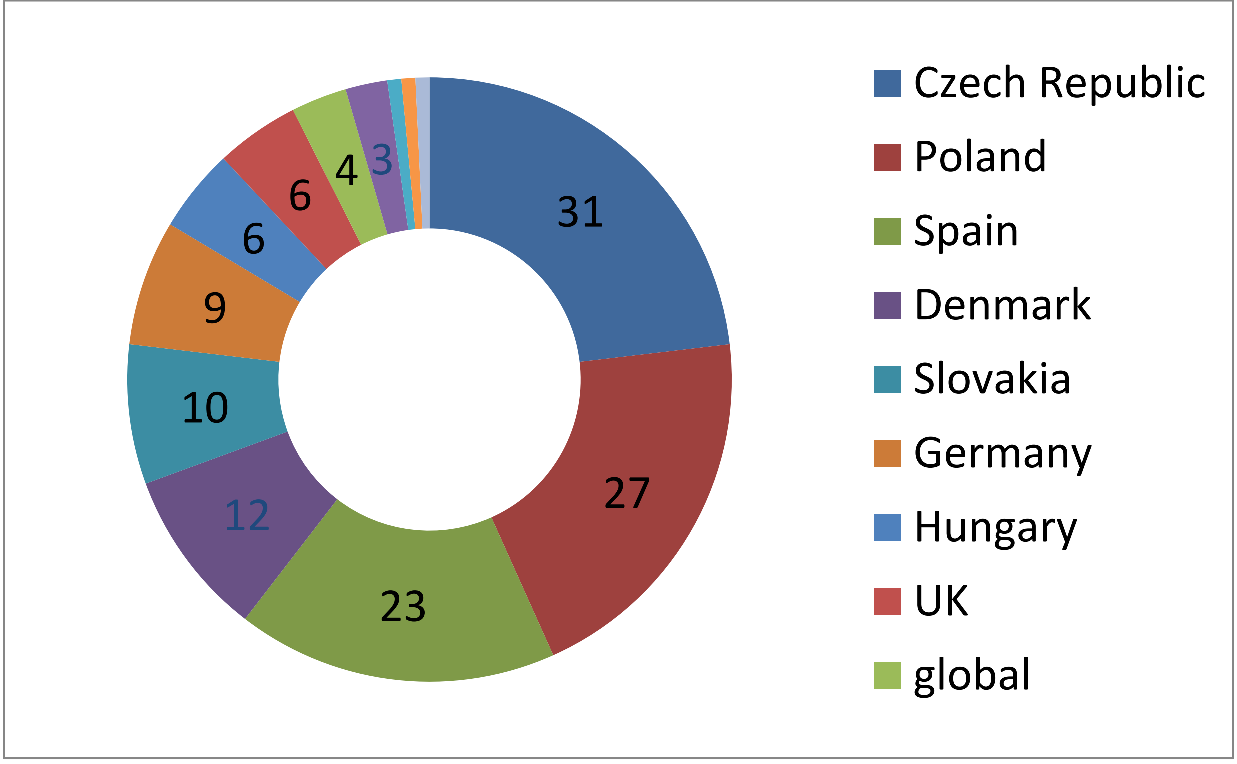
- Availability is the most reported and reports on availability are guaranteed by 75% of the contracts.

- Results of the performed penetration tests are reported in 71% of the cases.

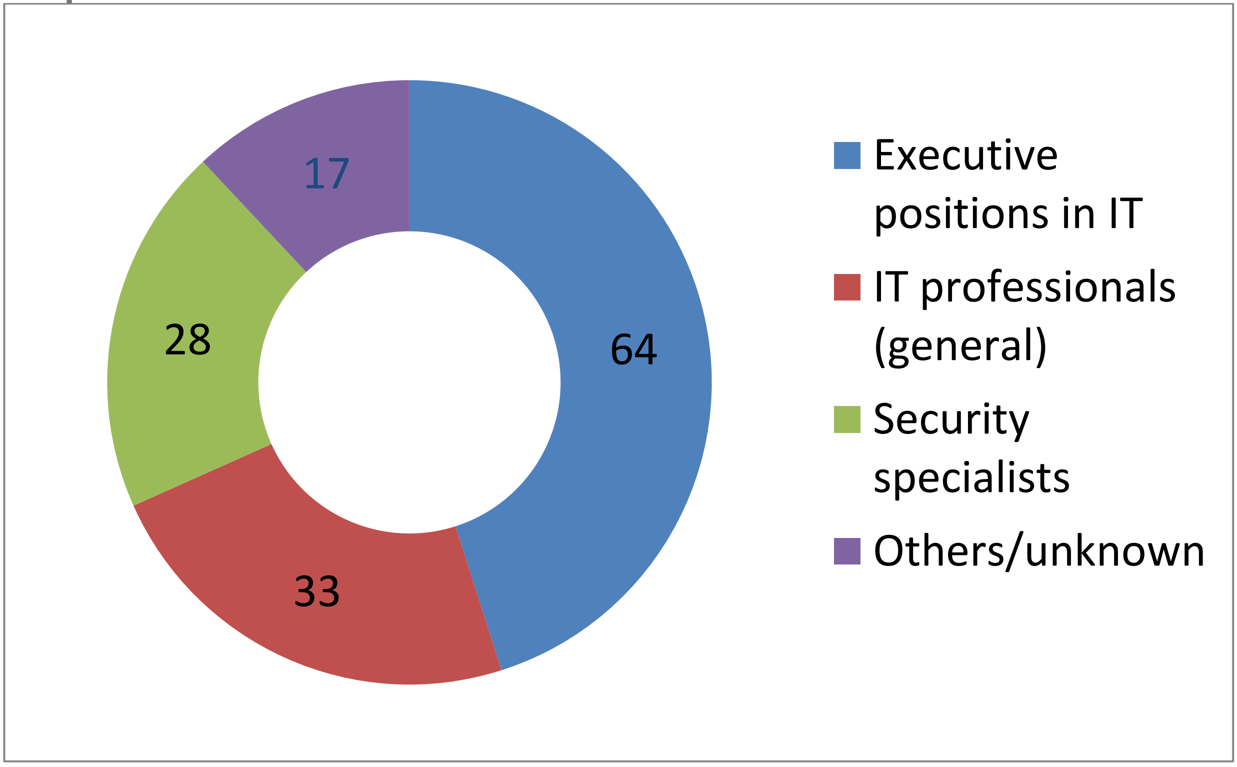
- Failover and backup system test and unit tests are reported in 67%.

Survey Results

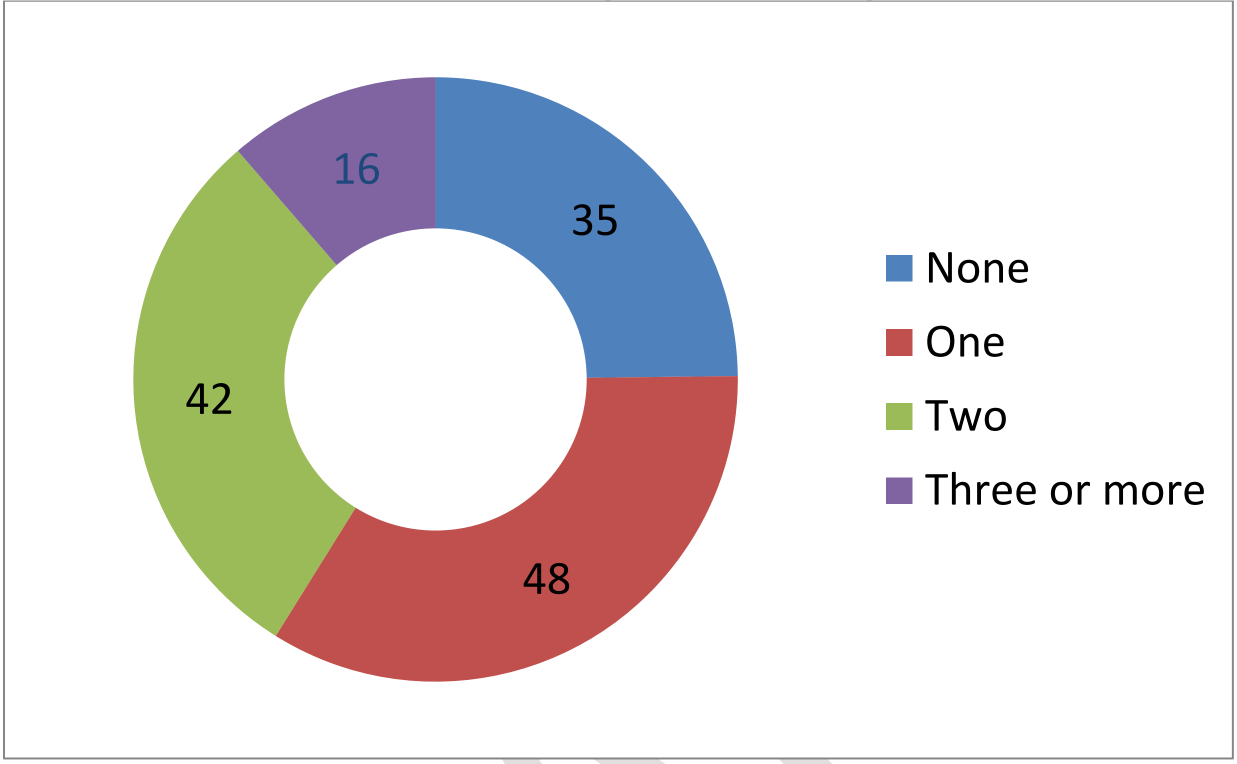
Respondent distribution - Country



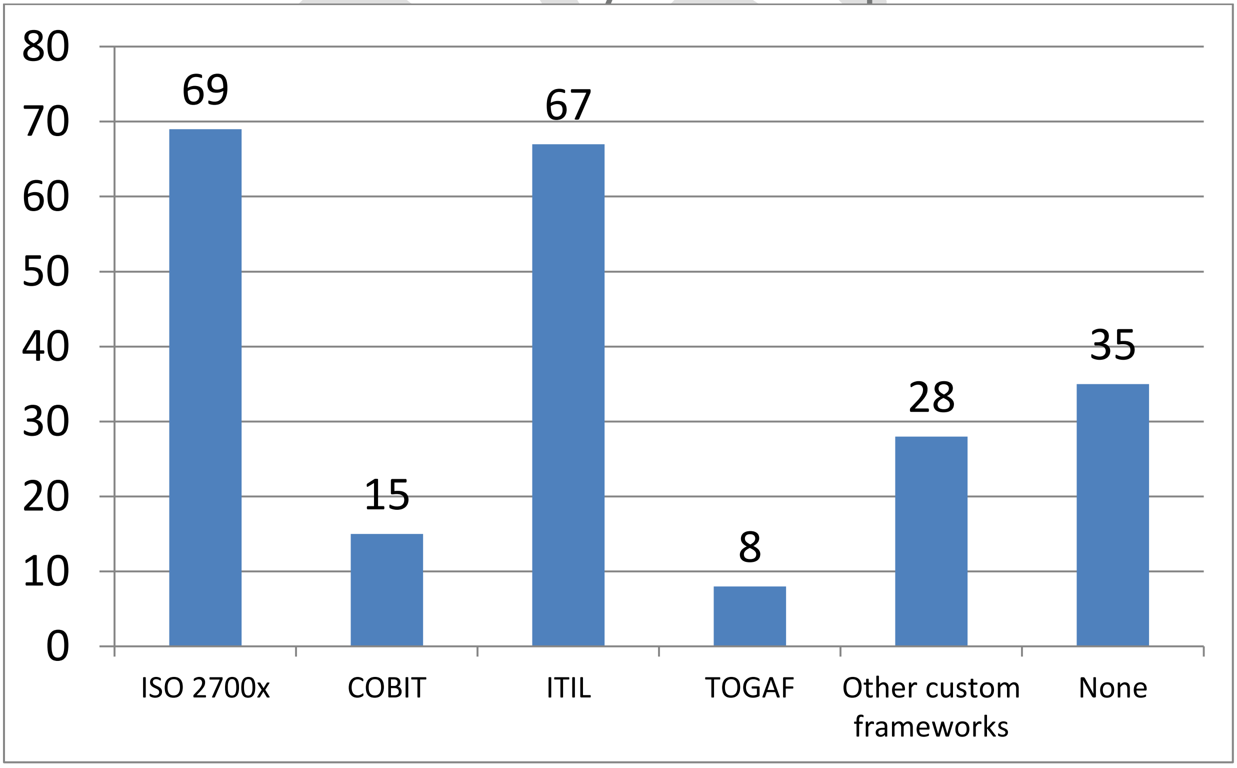
Respondent distribution - Professions



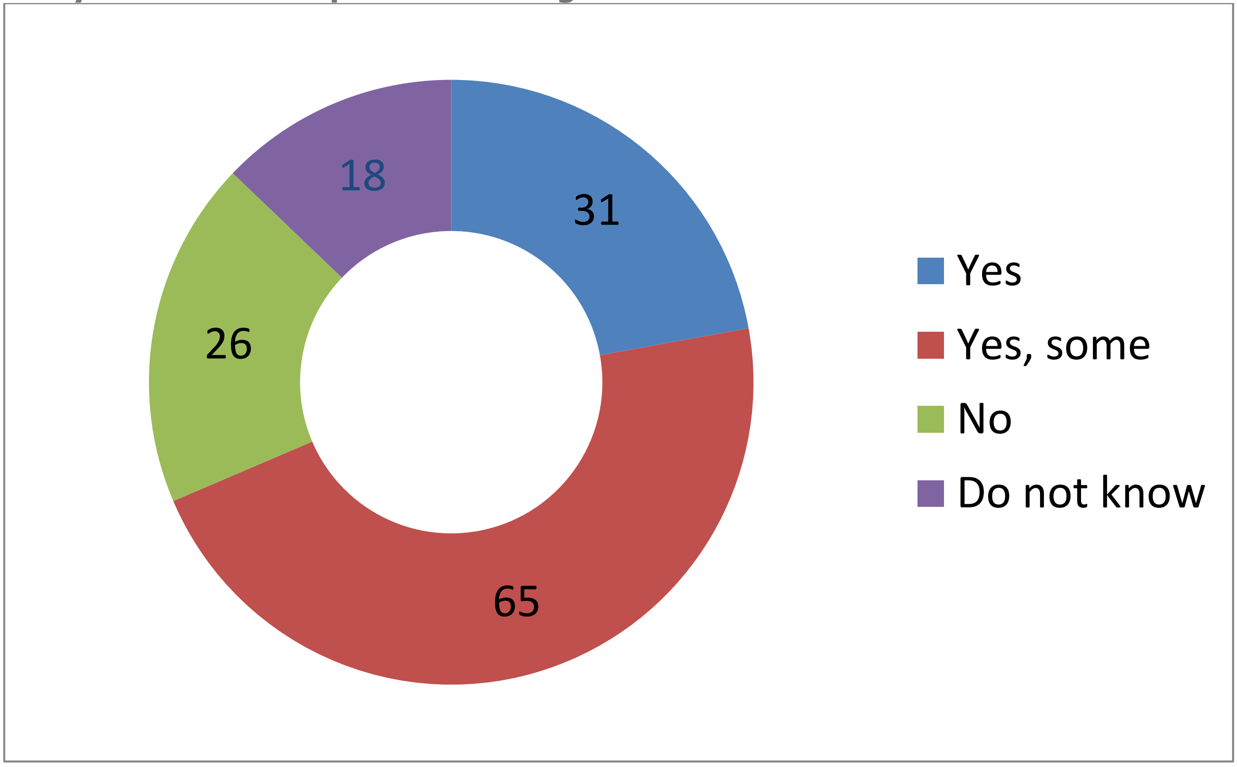
Governance frameworks and security standards adoption



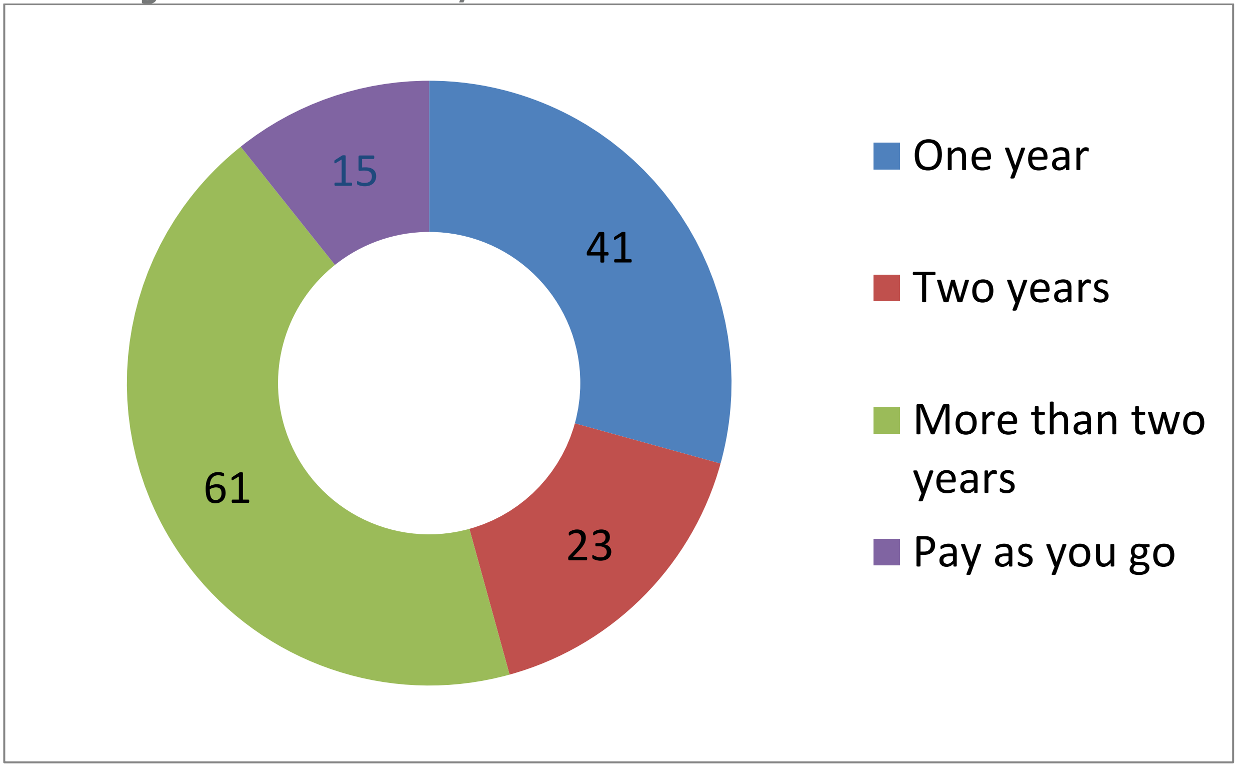
Governance frameworks and security standards adoption



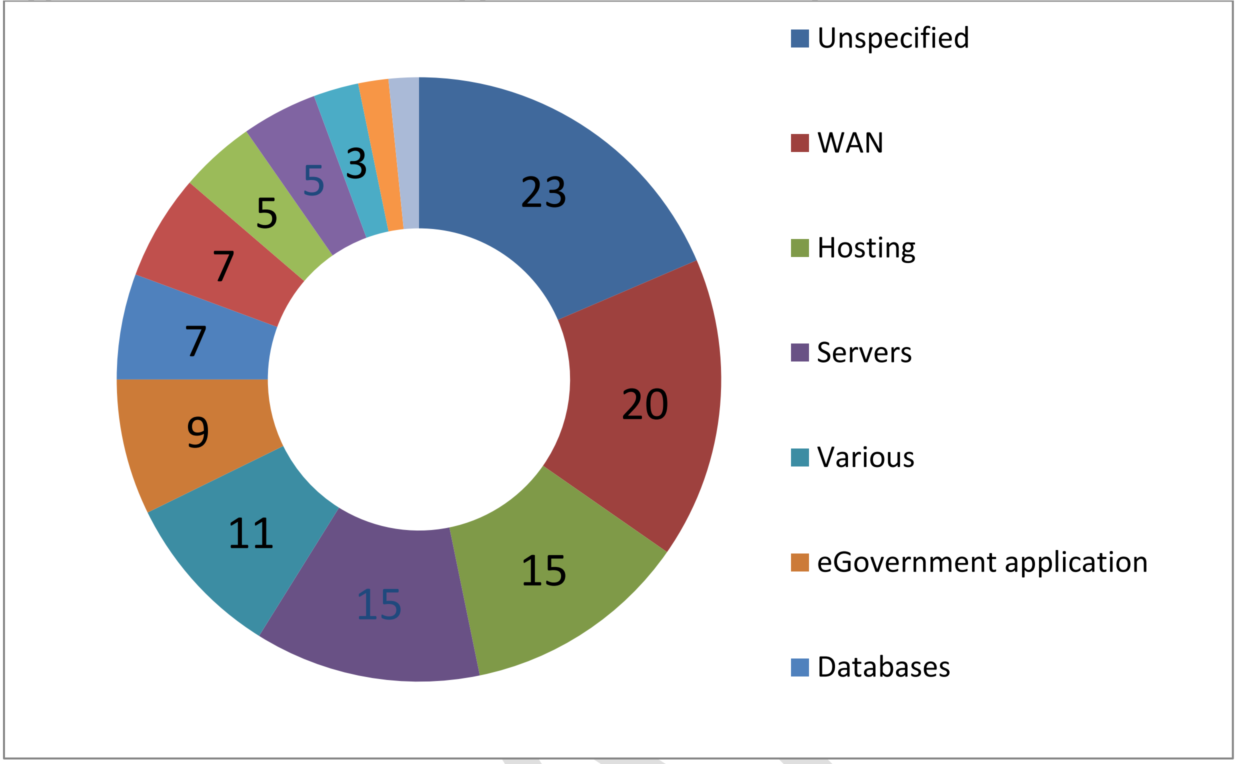
Are your IT service providers obliged to adhere to these standards too?



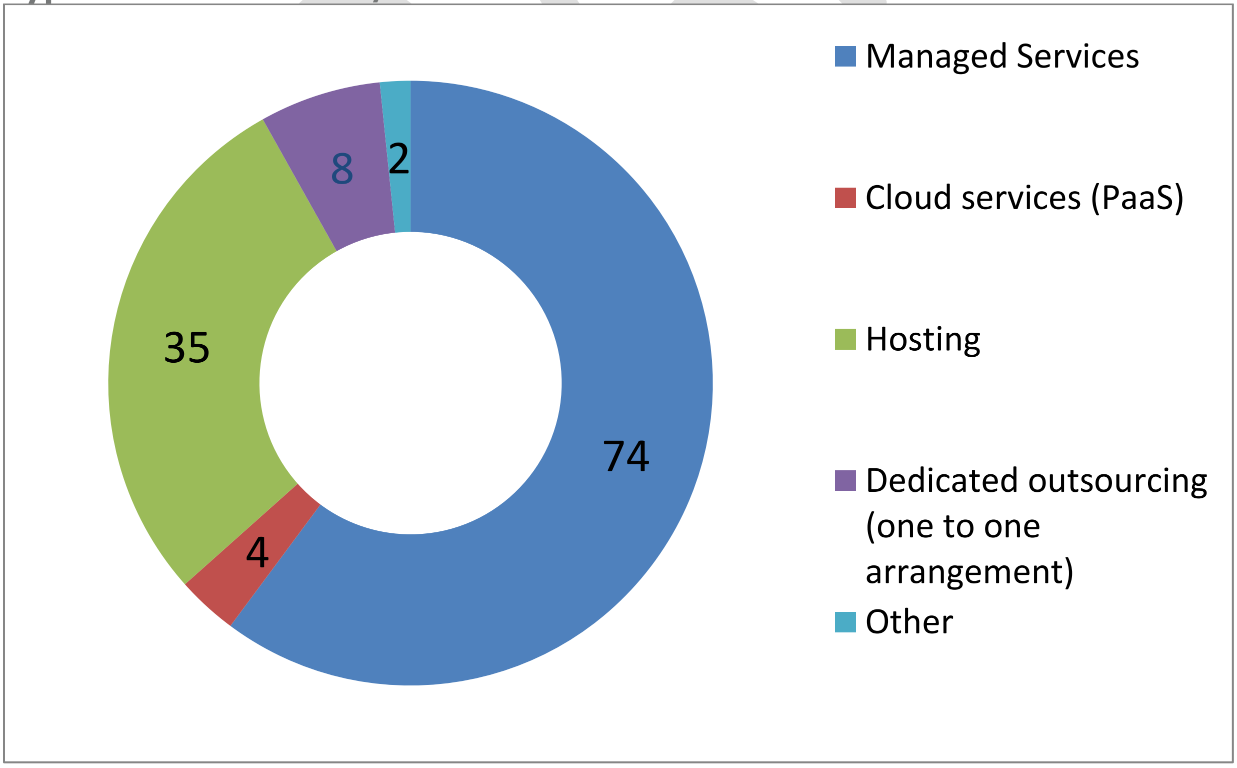
How long does the contract/SLA last?



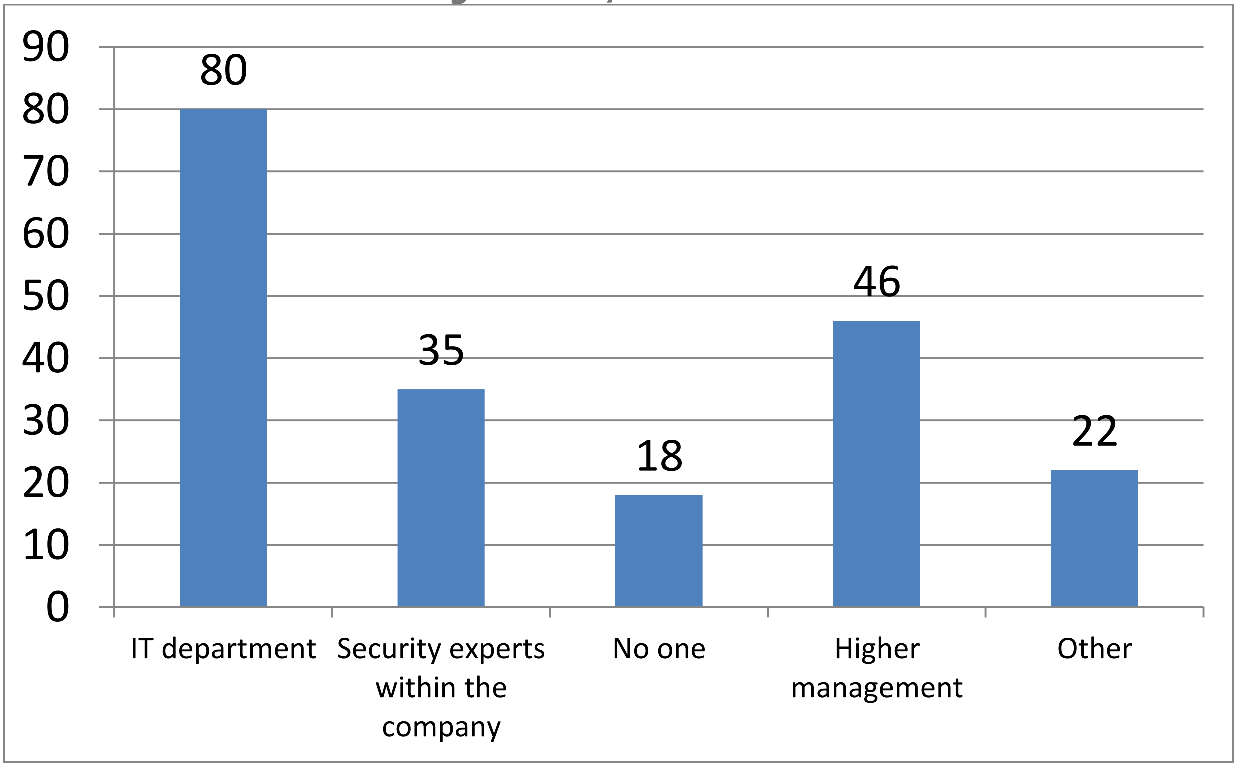
Types of infrastructure or applications covered by the SLA/contract



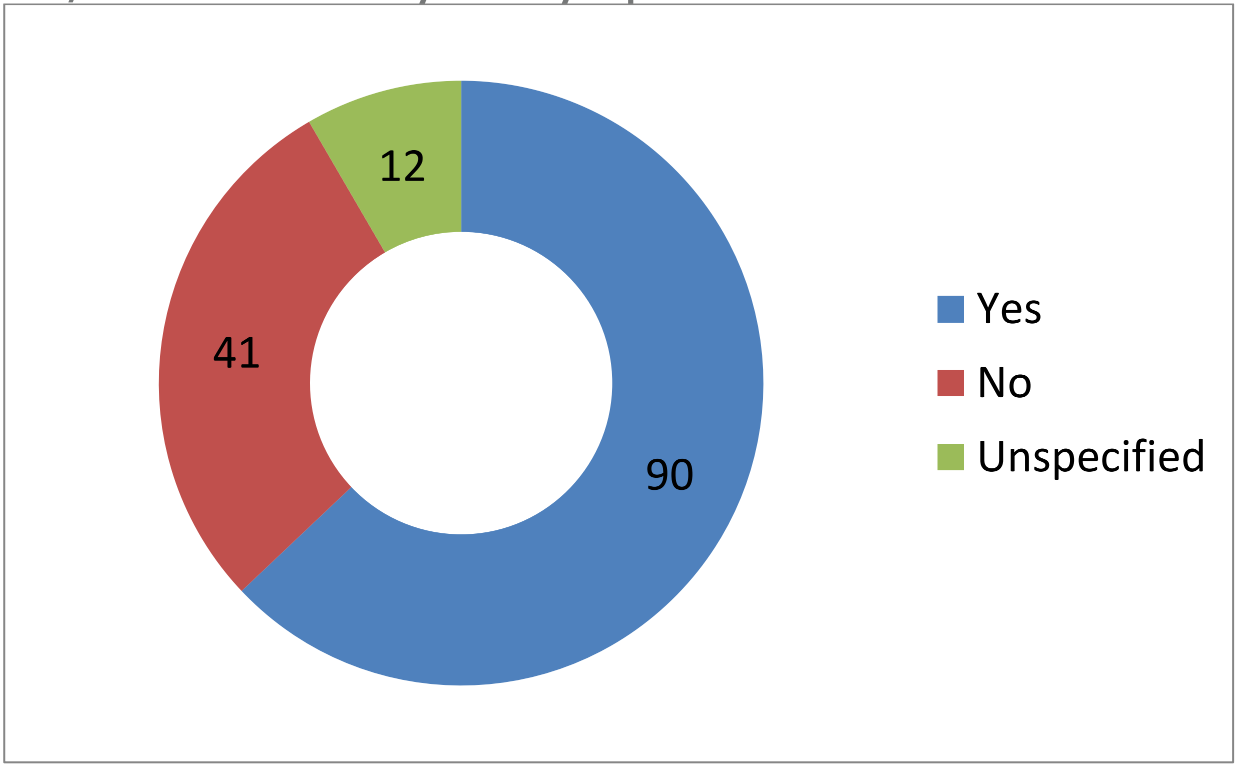
Types of the contracts/SLAs



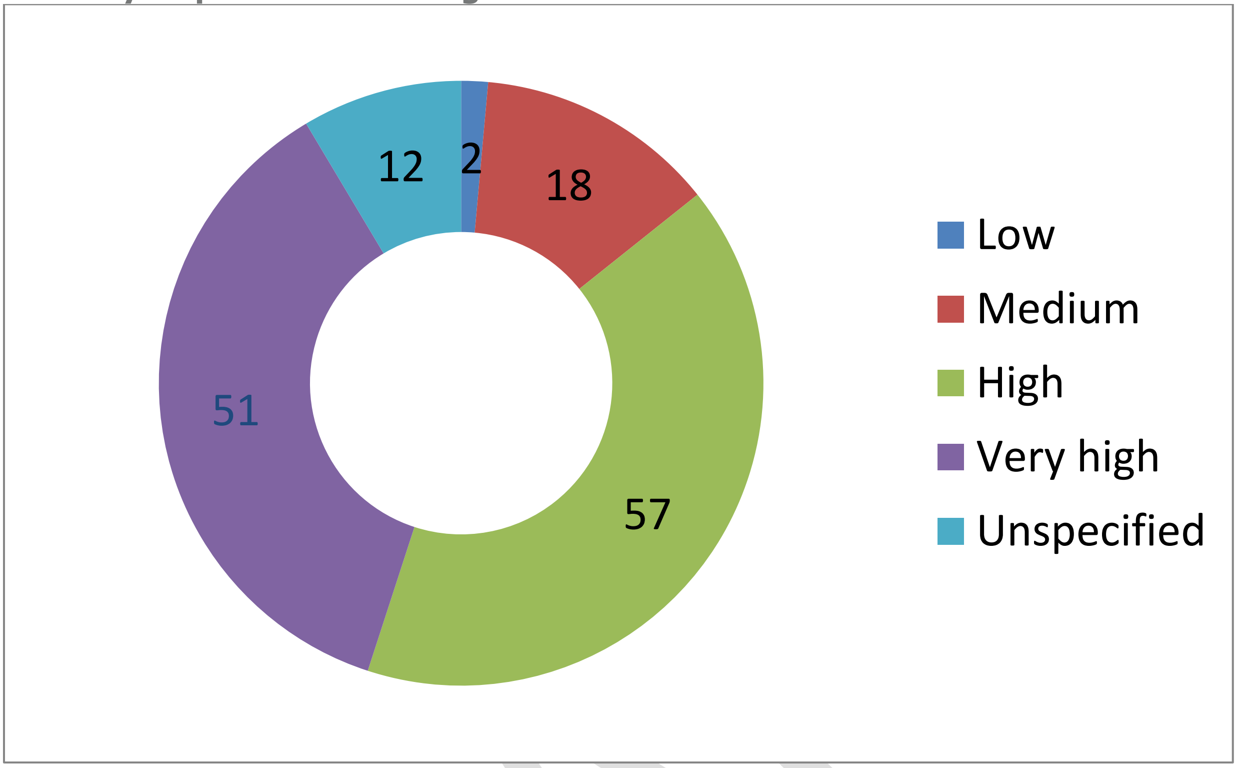
Who was involved in setting the SLA/contract



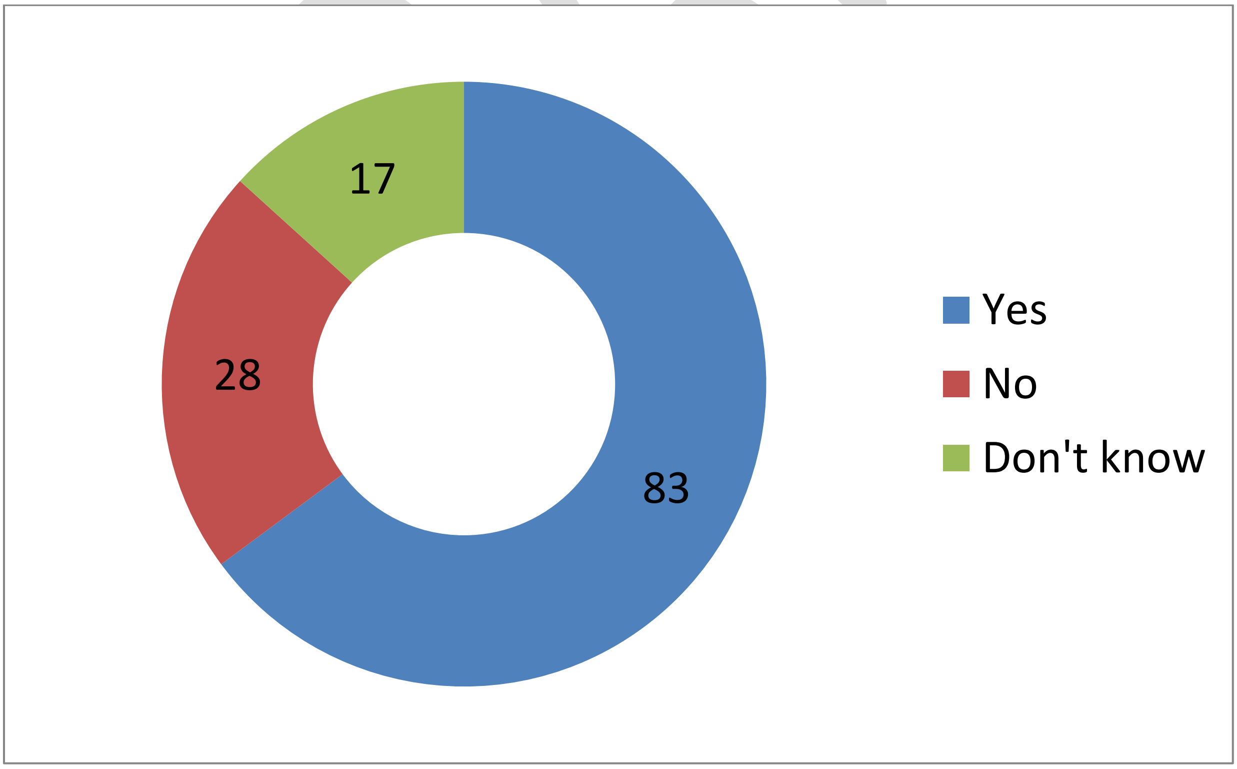
SLA/contract reviewed by security experts



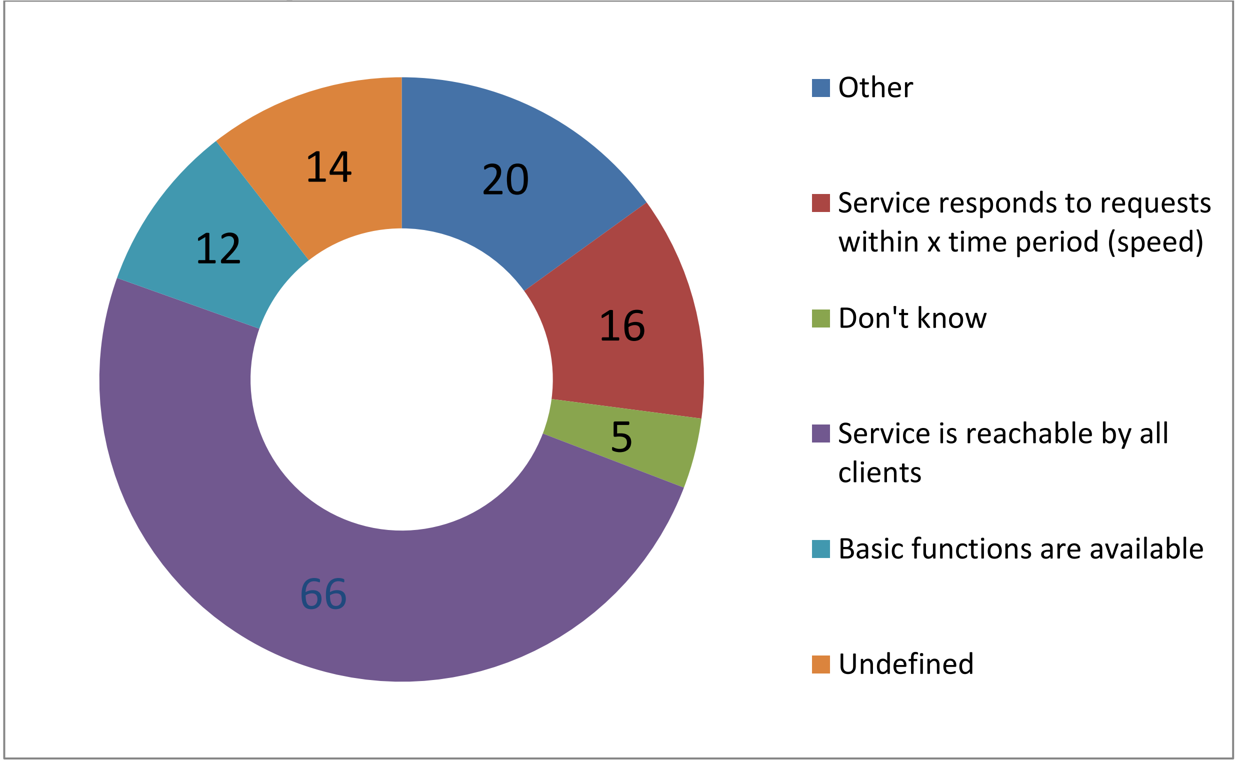
Security requirements rating



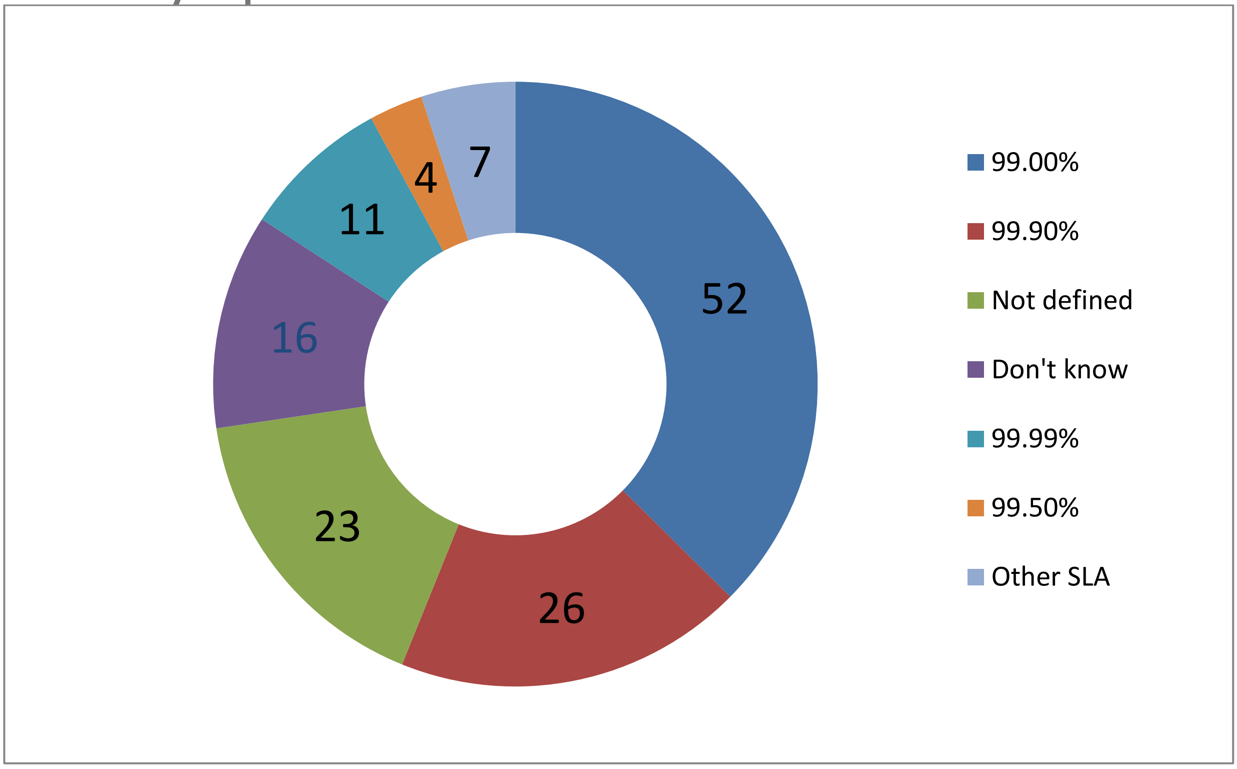
SLA defined



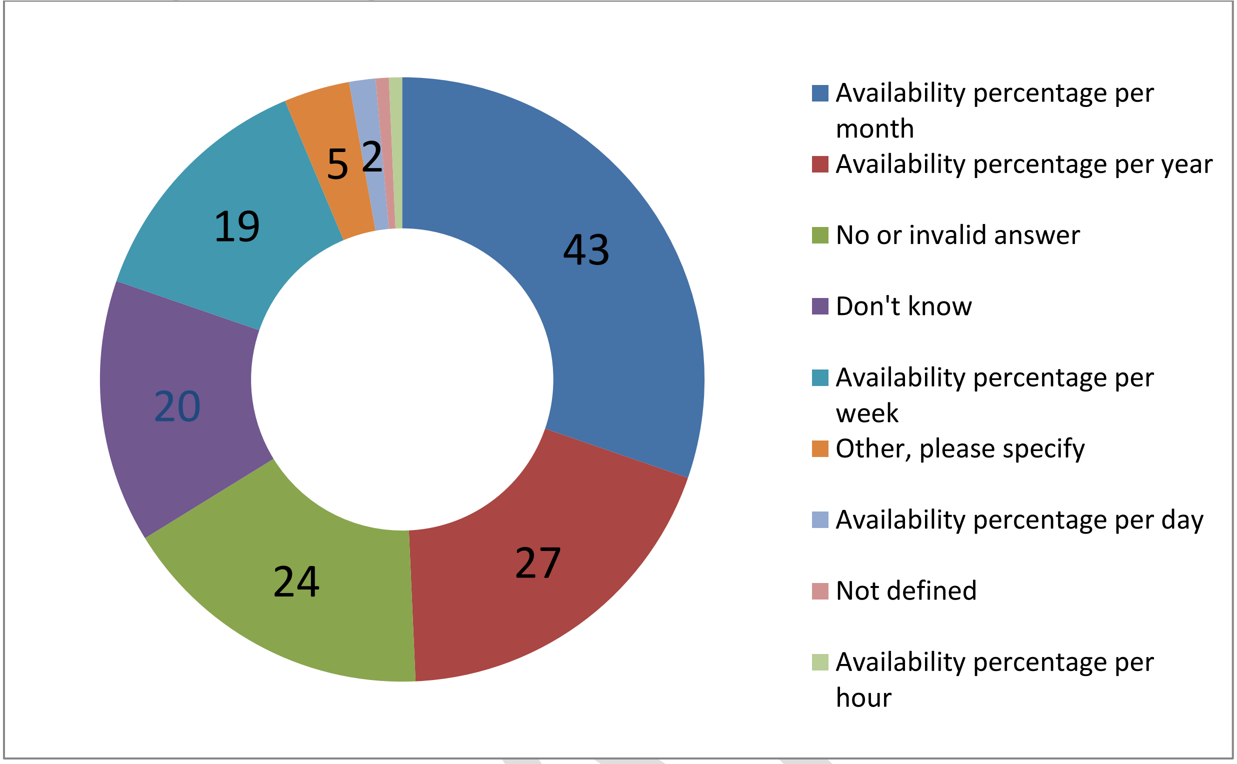
Define availability



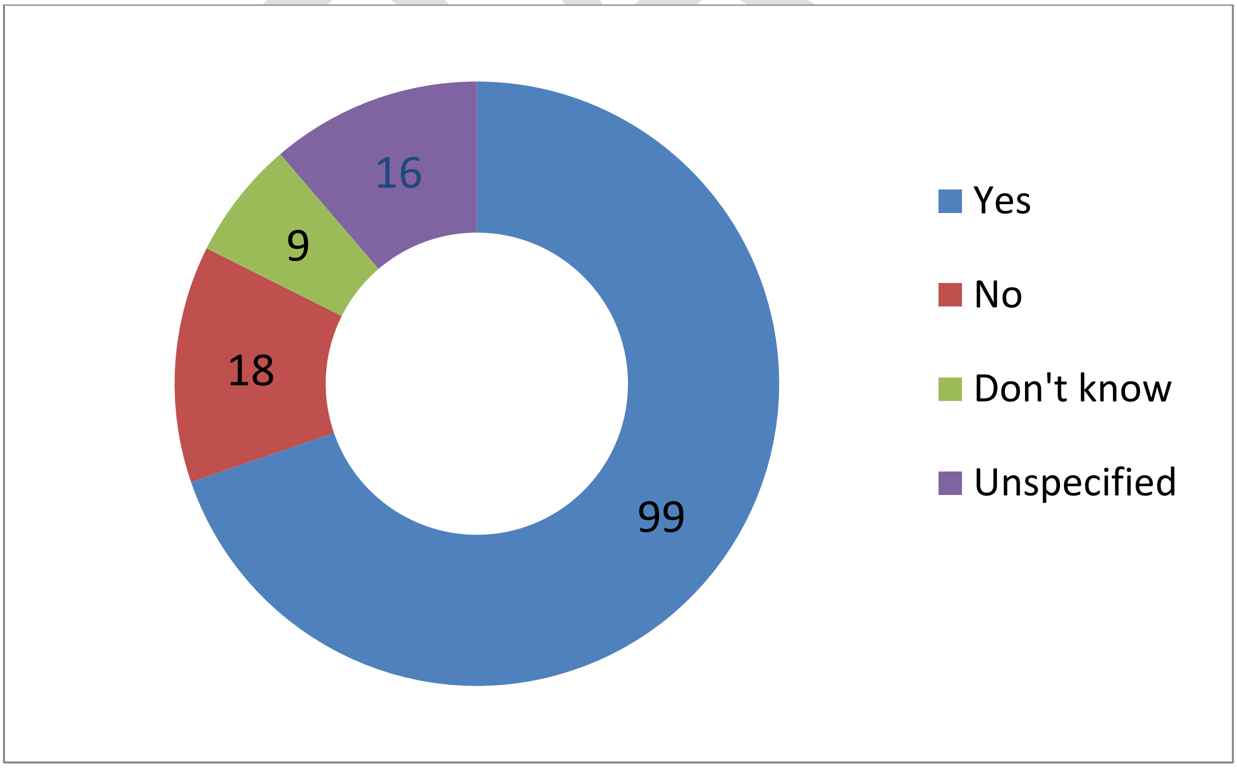
Availability requirements



Availability definition period



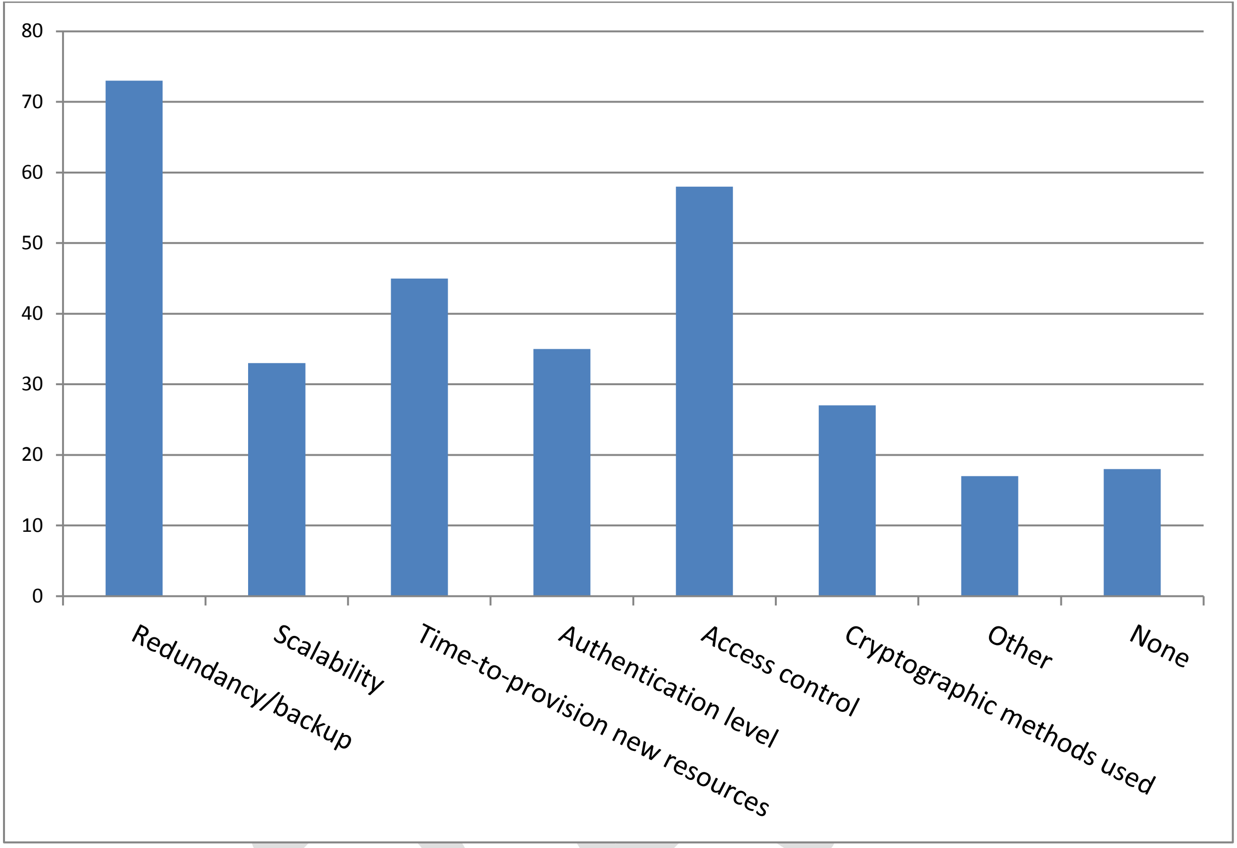
Is the service provider obliged to report downtime within a certain time frame?



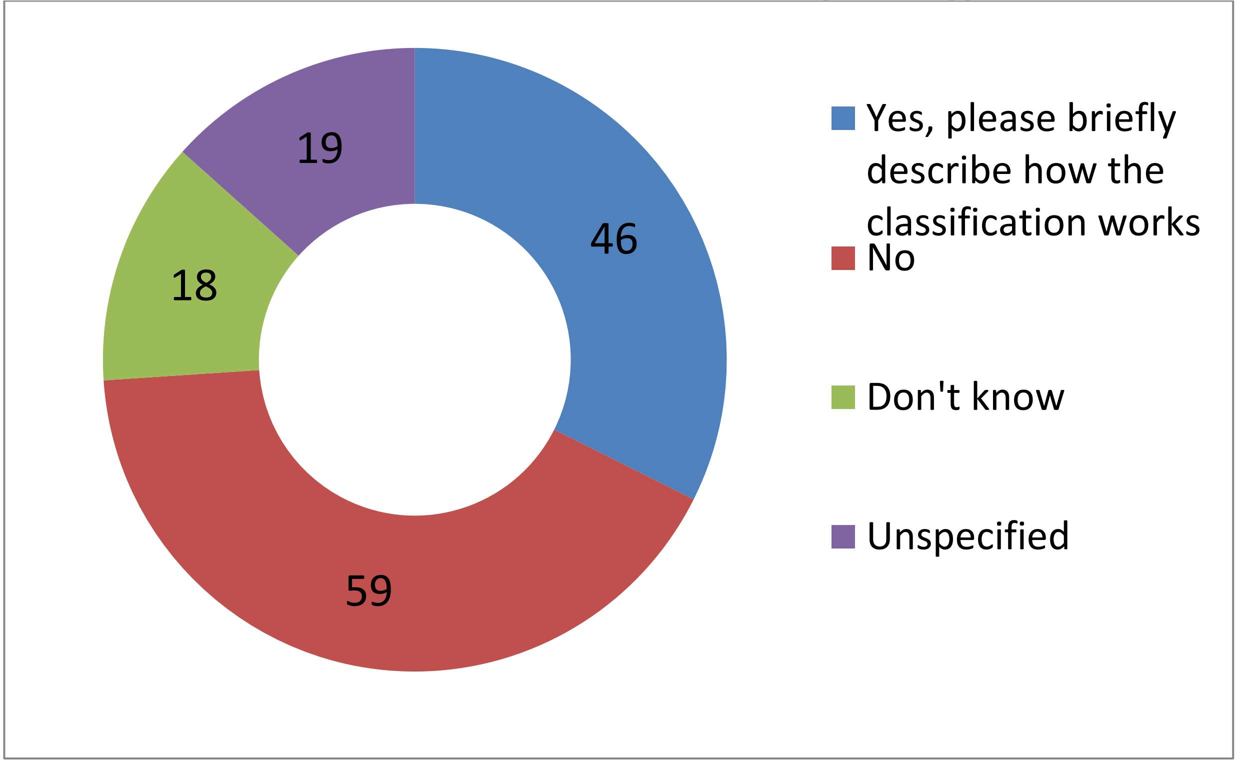
Statements concerning availability

- We monitor availability of the service in ENISA as well
- We would advise vendor if application unavailable or unstable
- Almost no flexibility exists
- Very important criterion
- Penalties for non-availability, a strict requirement to keep two separate routes and separate technical appliances
- Overrated - integrity more important
- Similar SLA parameters are concluded on a central Internet connectivity.
- Availability is calculated in hours, 1 year = 8640 h
- There are set times (in hours) to start removing failure and restoration operations
- Institute has not set uniform availability for all systems, availability are distinguished according to the criticality of the system
- Services covered by this contract have basic availability requirements, the corporate site is hosted and followed in another contract with another provider
- We are considering that we will operate the service ourselves

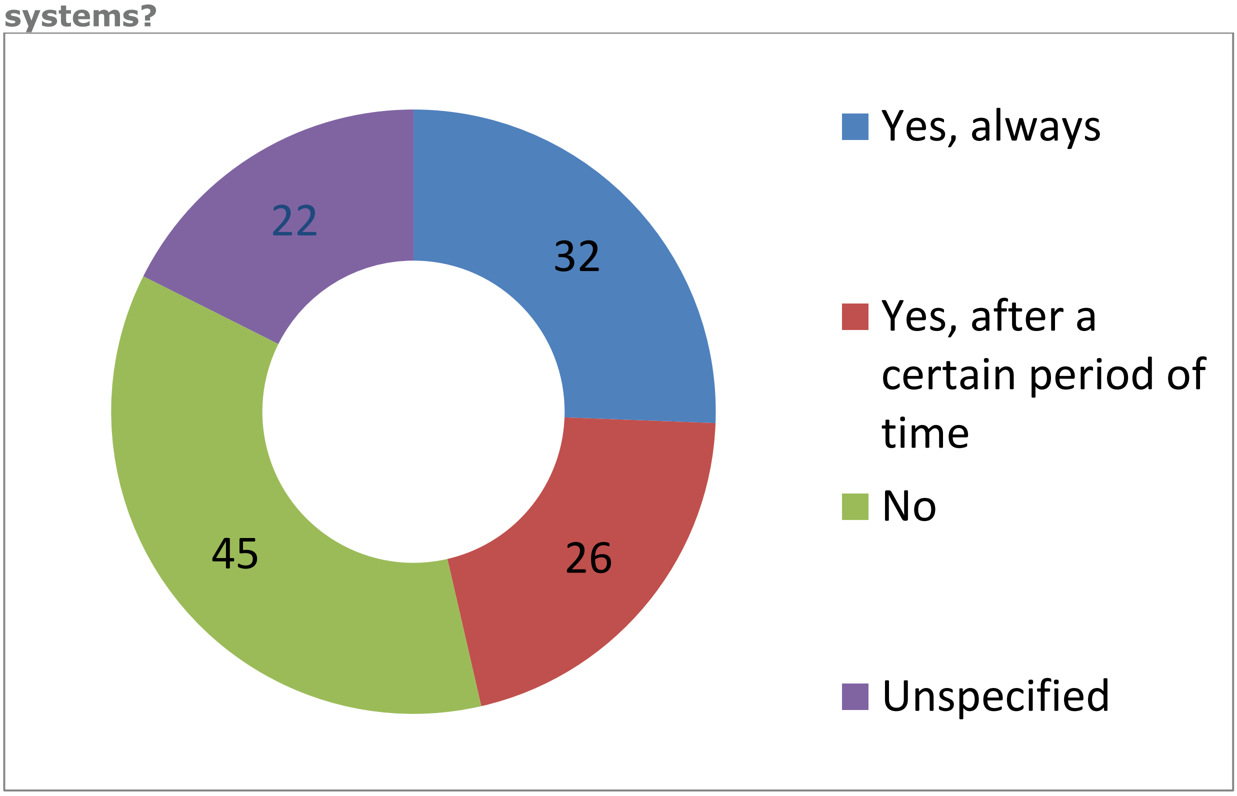
Which of the following aspects did you explicitly address in your SLA/contract?



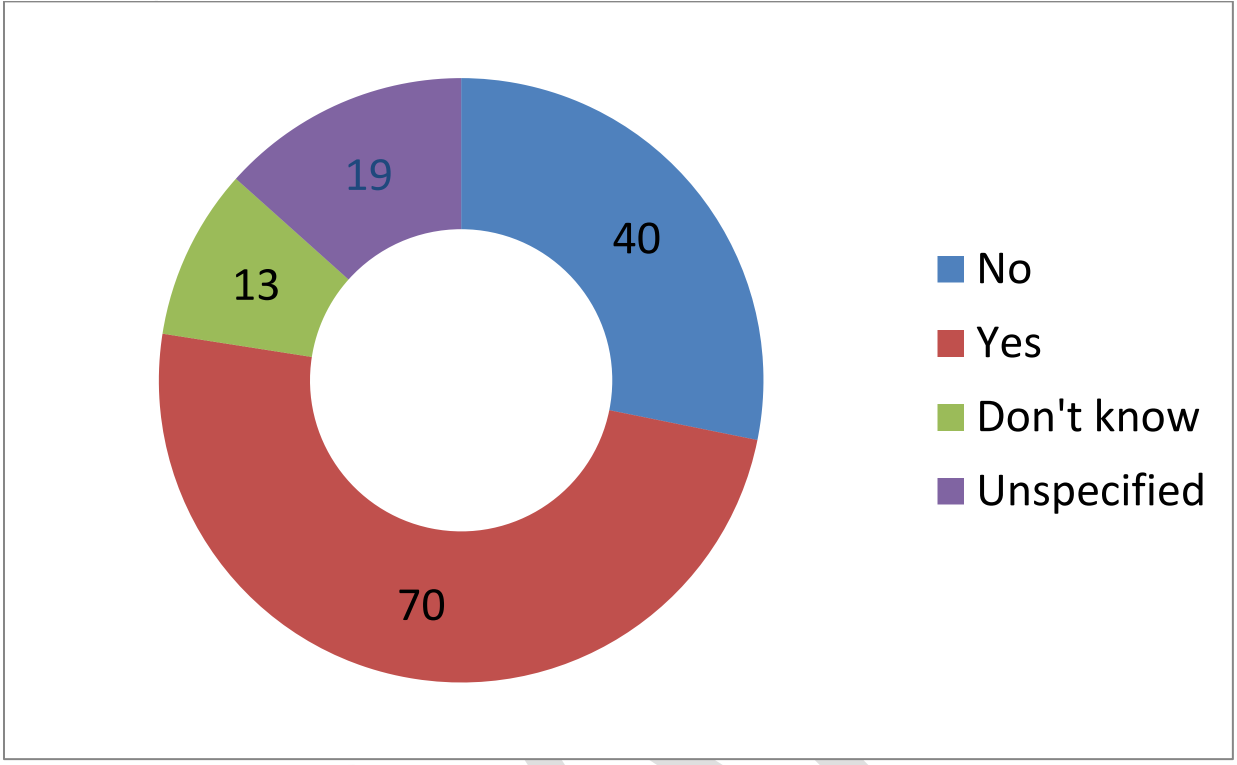
Does the SLA/contract include a classification of (security) incidents?



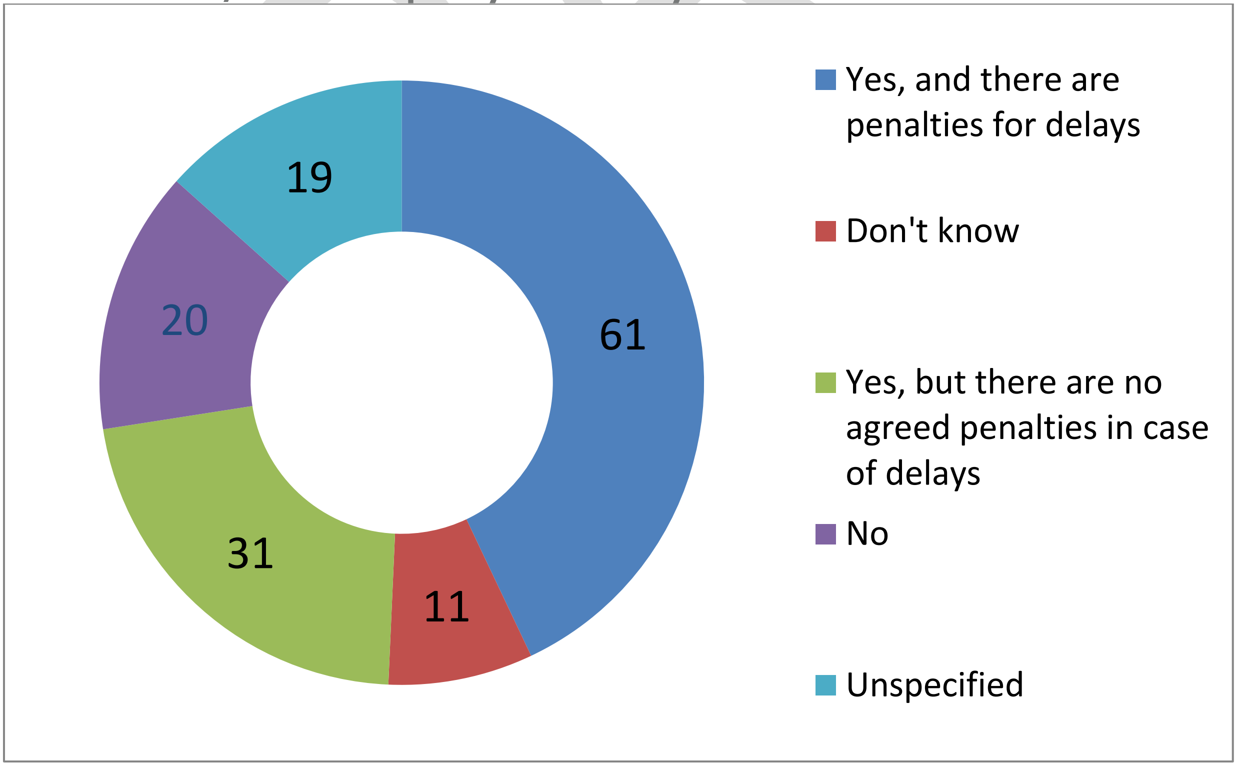
Does the definition of security incidents include incidents to secondary systems?



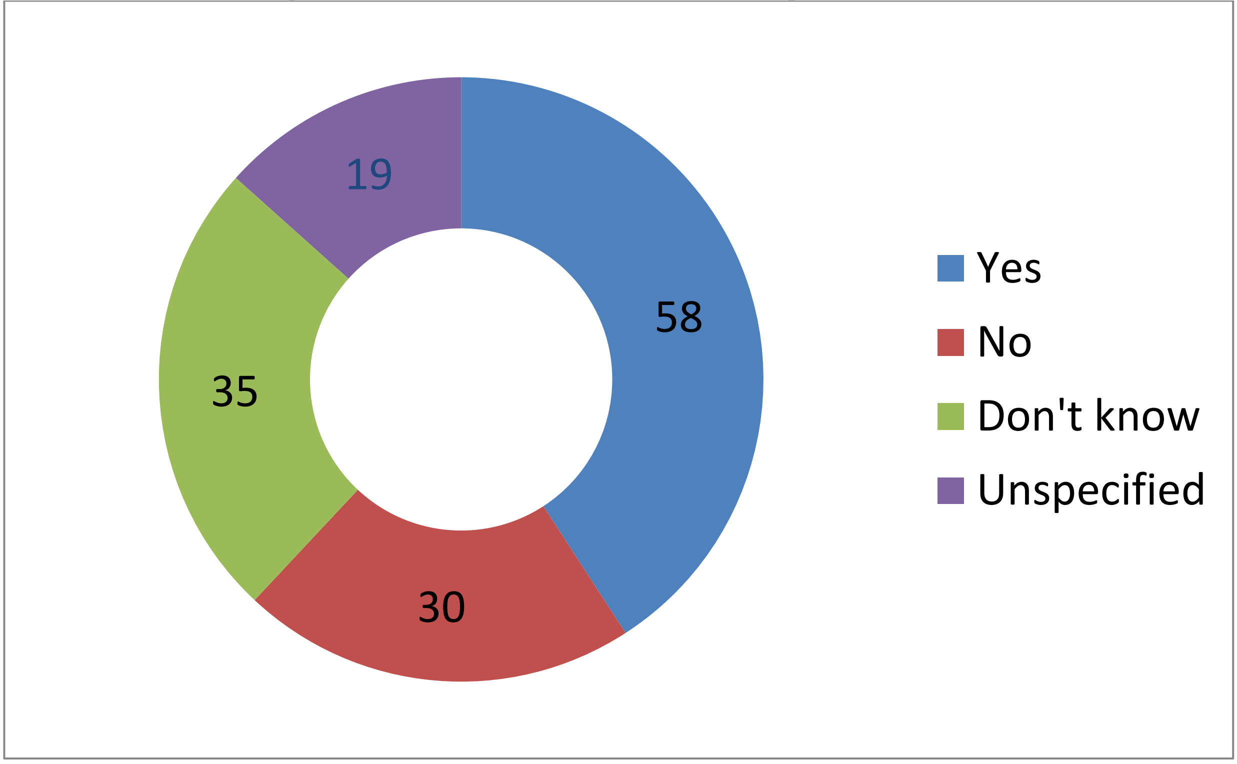
Does the SLA/contract oblige the service provider to report security incidents, within a certain time frame?



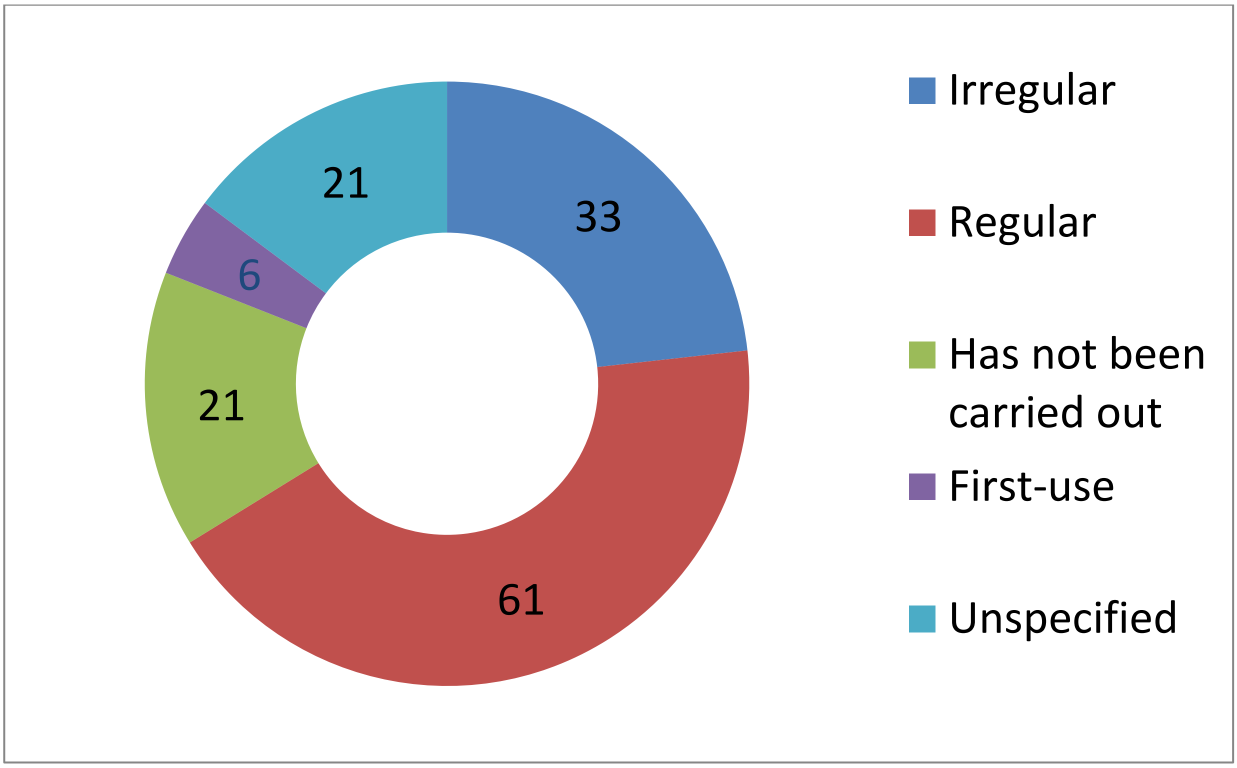
Does the SLA/contract specify a recovery time for incidents?



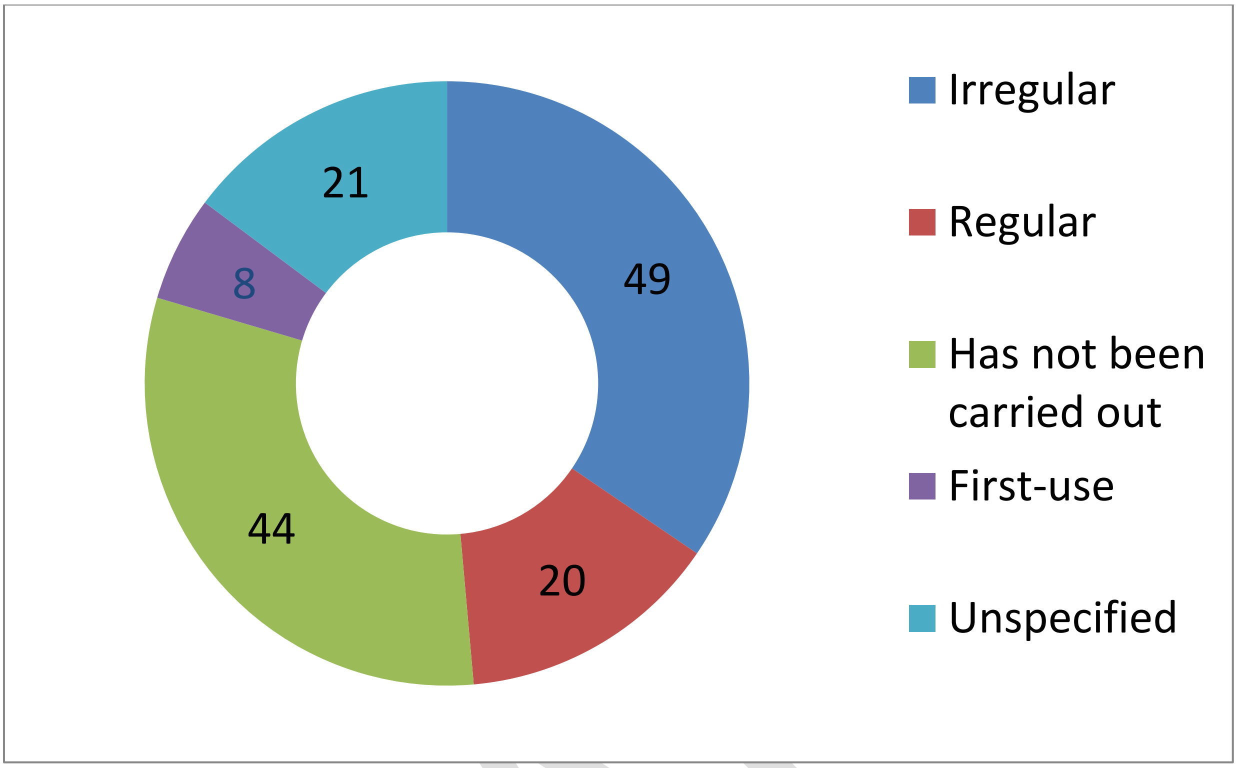
Does the service provider 'measure' the security of the service?



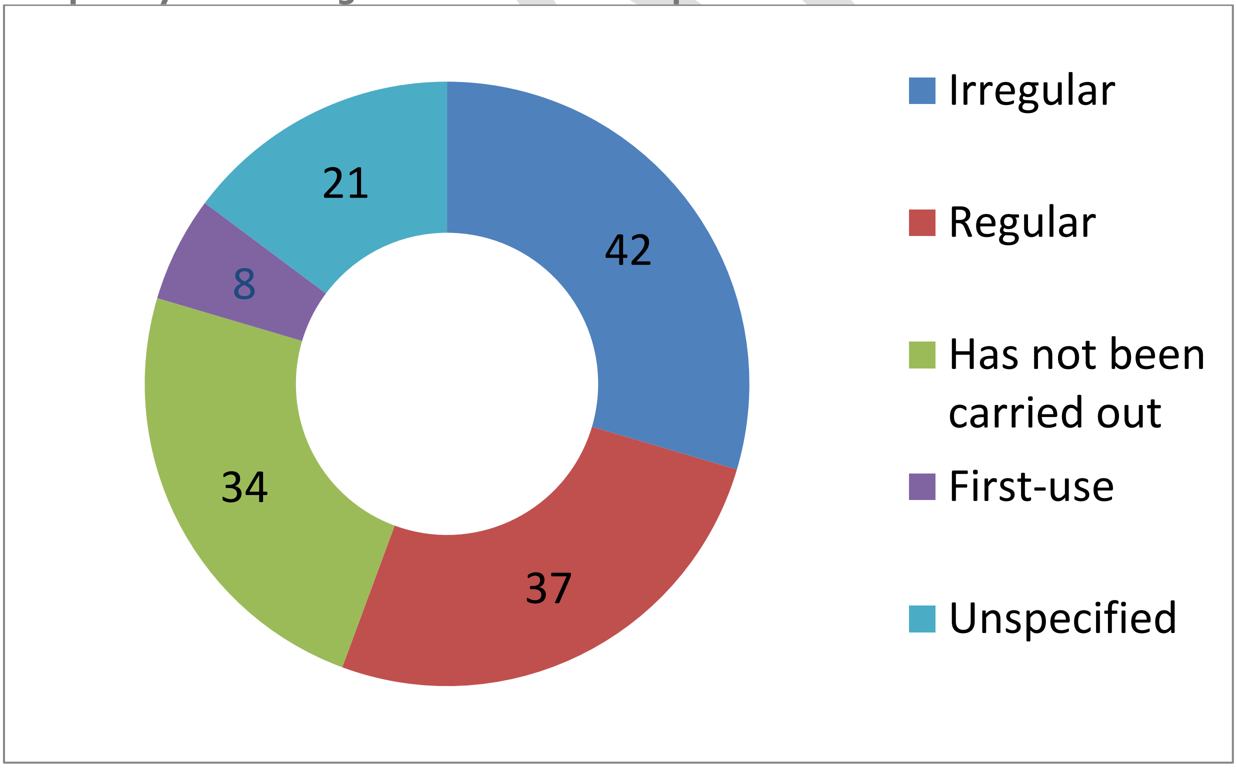
Testing frequency of availability



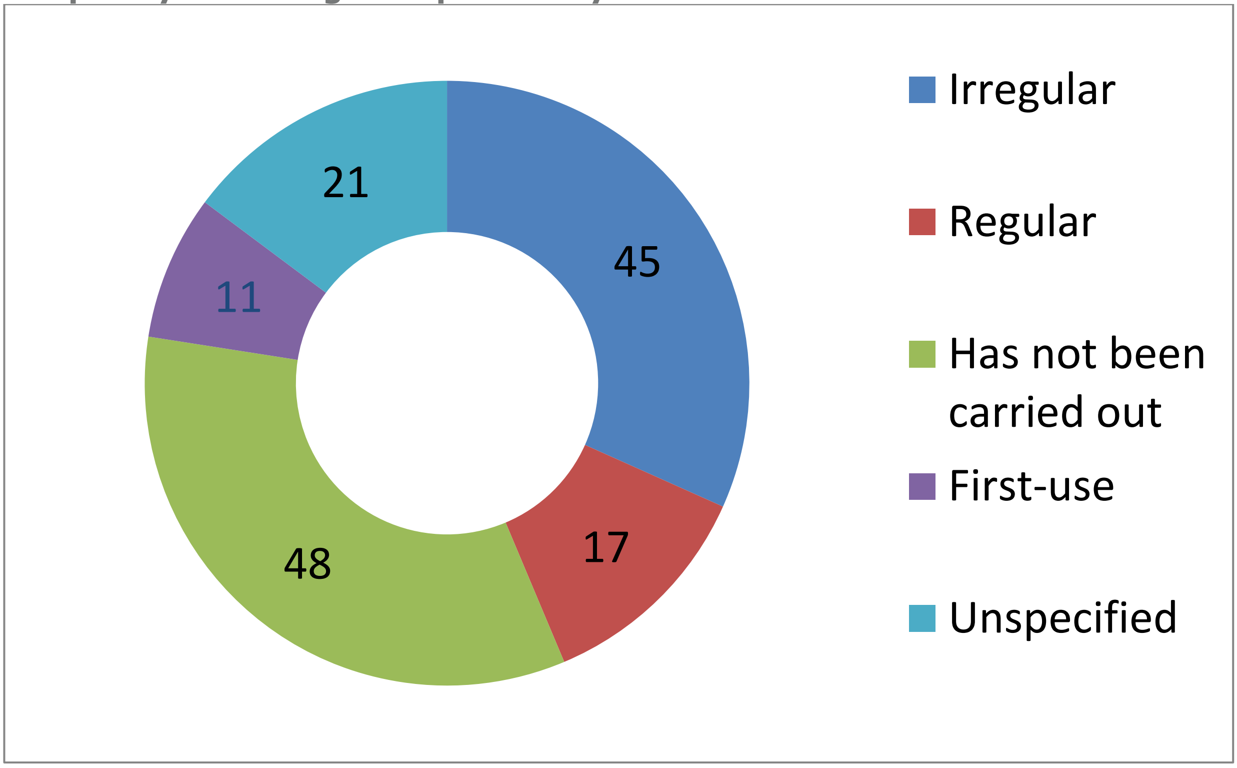
Frequency of running penetration tests?



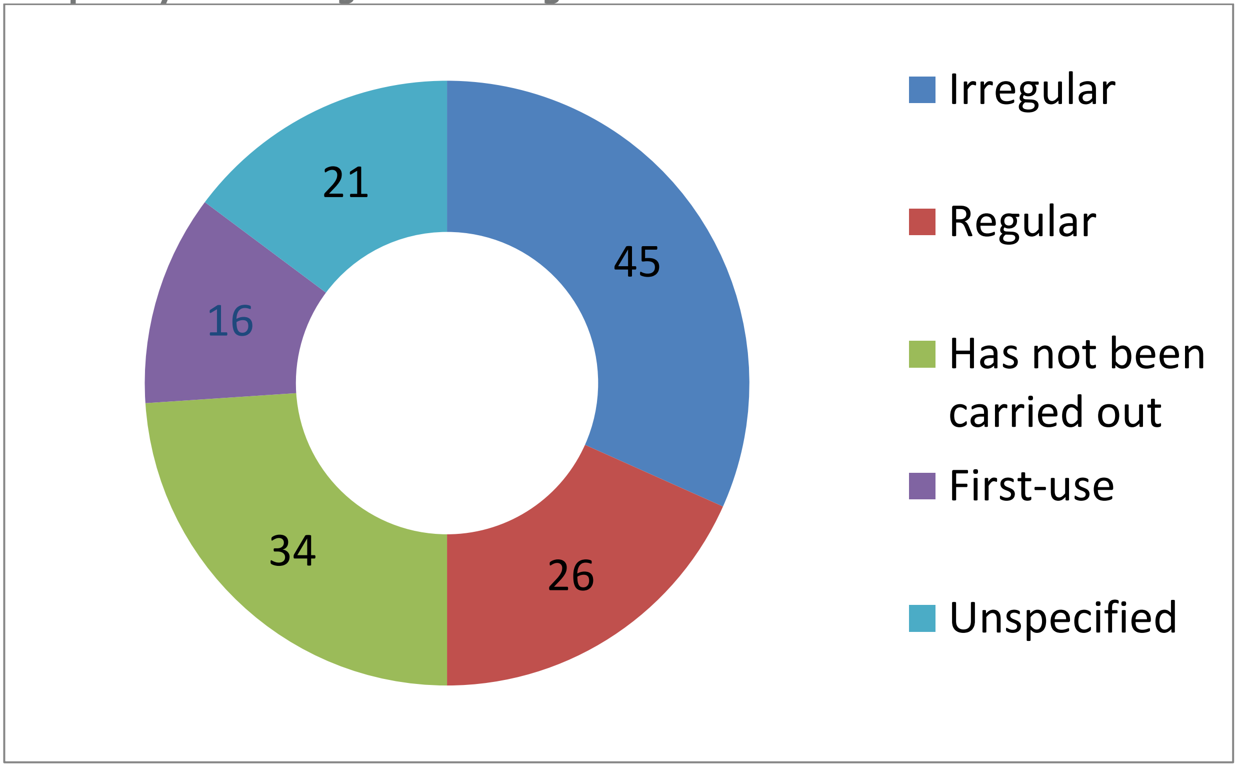
Frequency of running failover and backup tests?



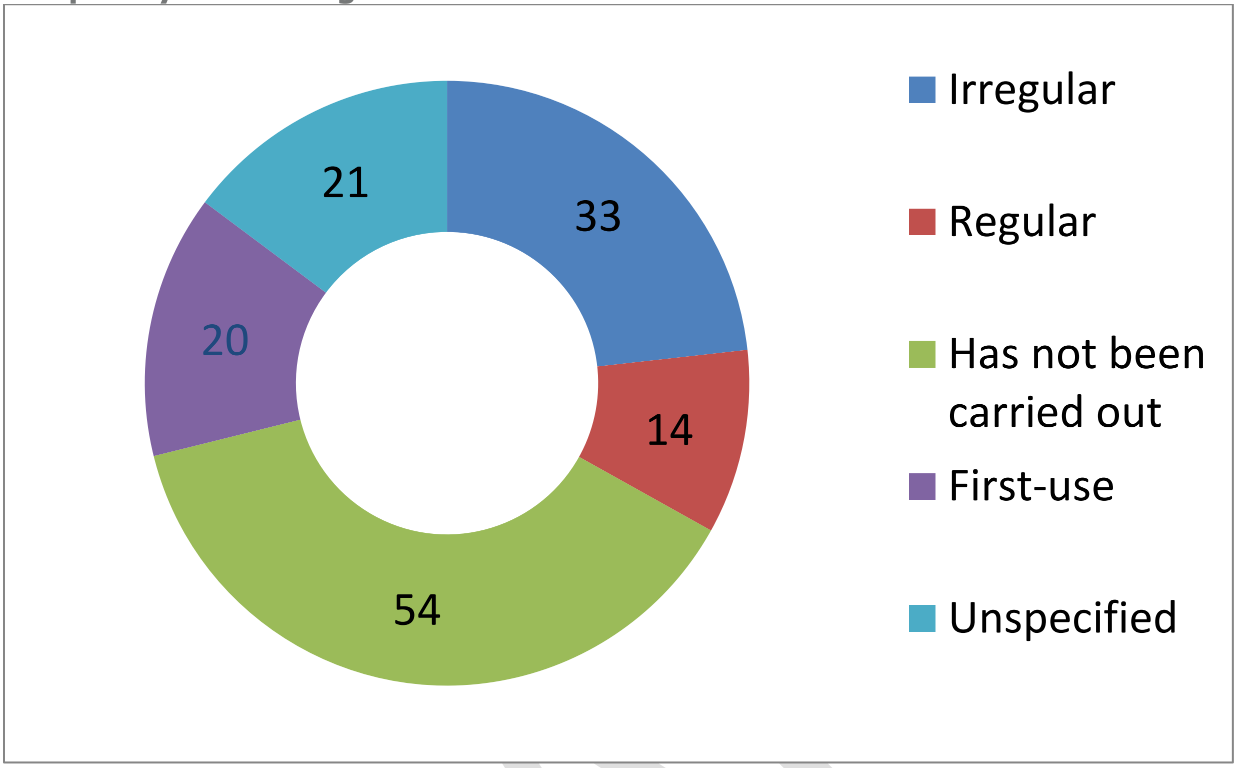
Frequency of testing data portability?



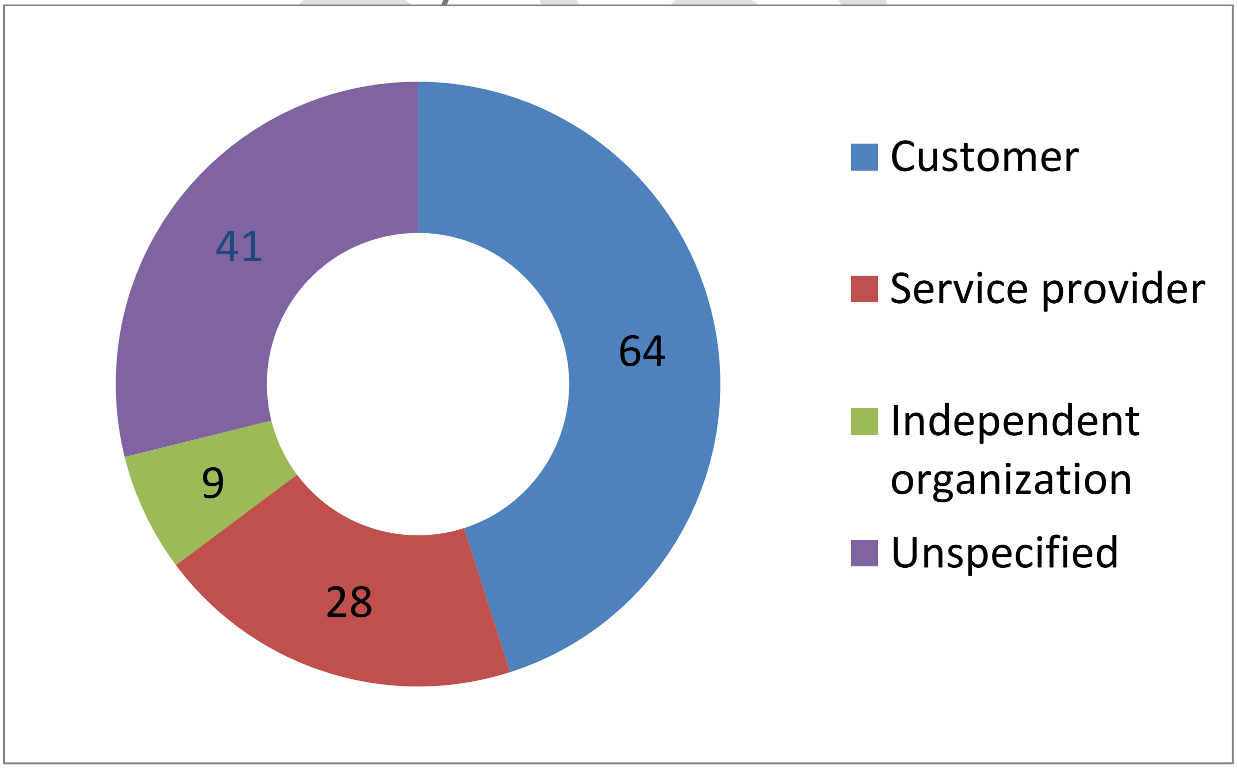
Frequency of running load testing?



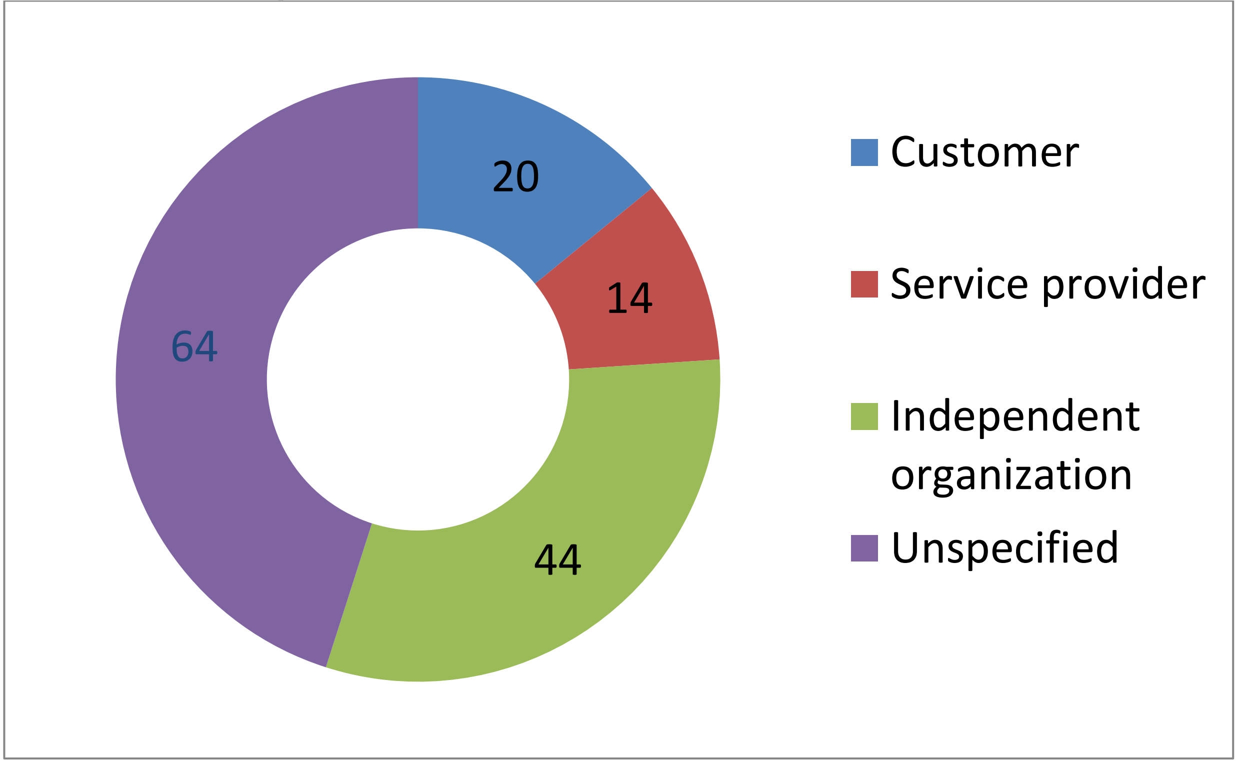
Frequency of running unit tests?



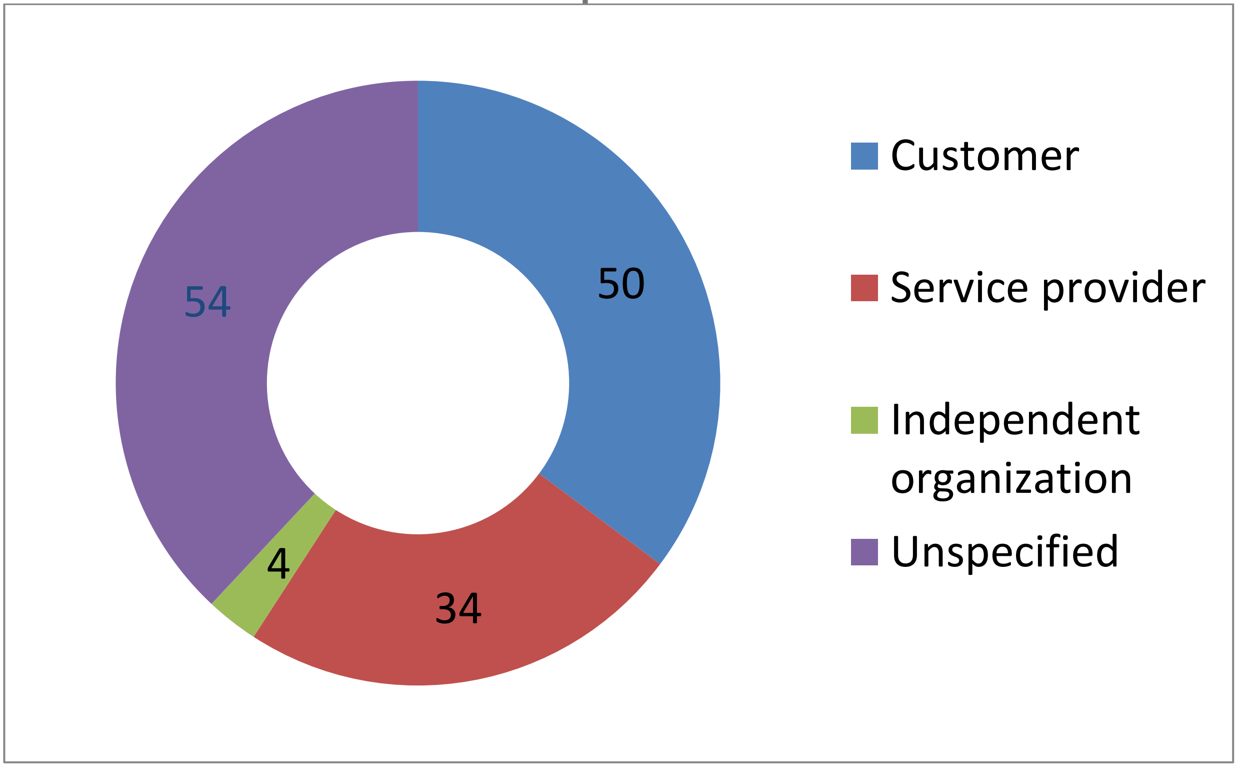
Who carries out availability measurement?



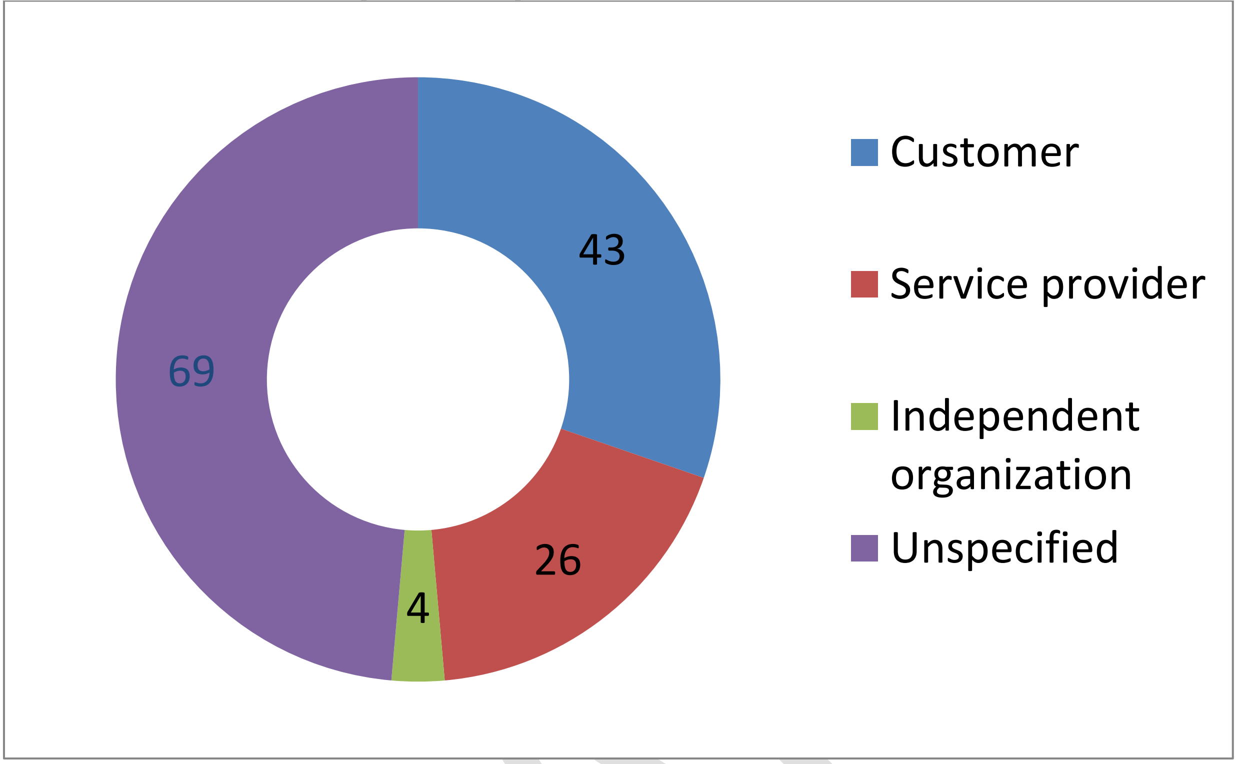
Who carries out penetration tests?



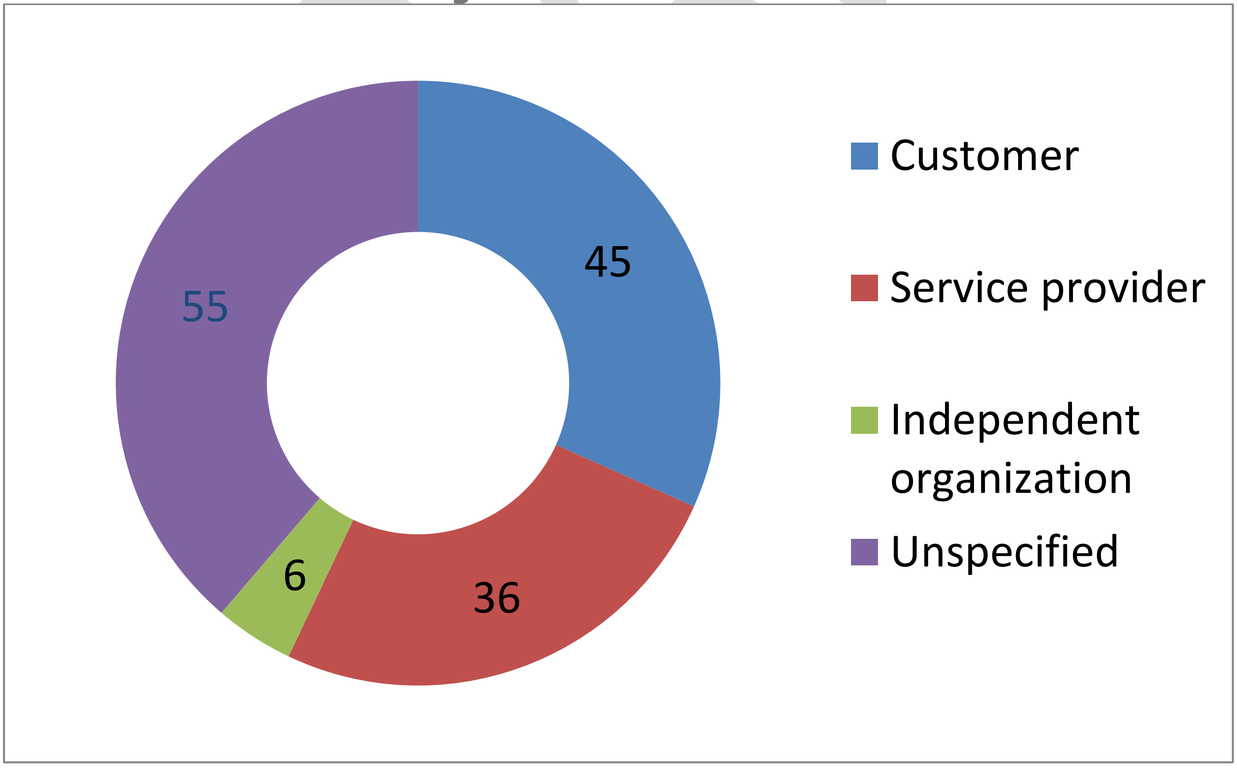
Who carries out failover and backup tests?



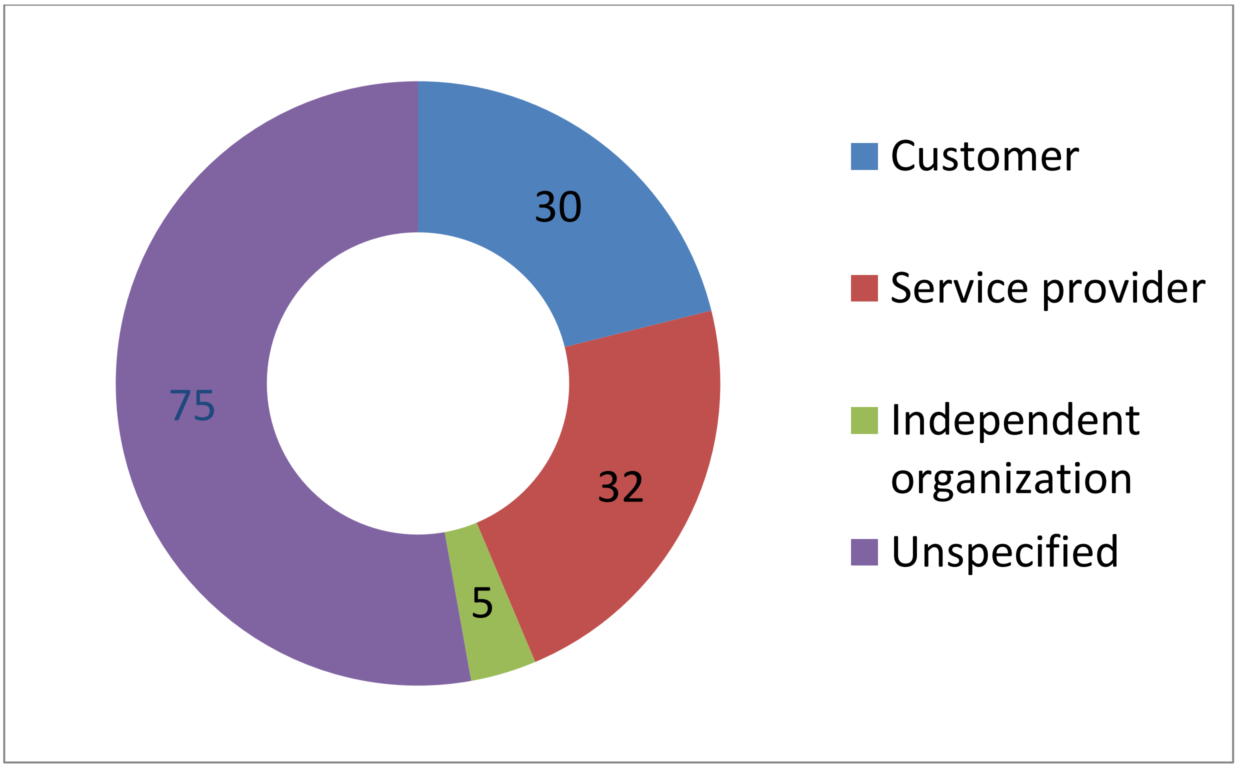
Who carries out data portability tests?



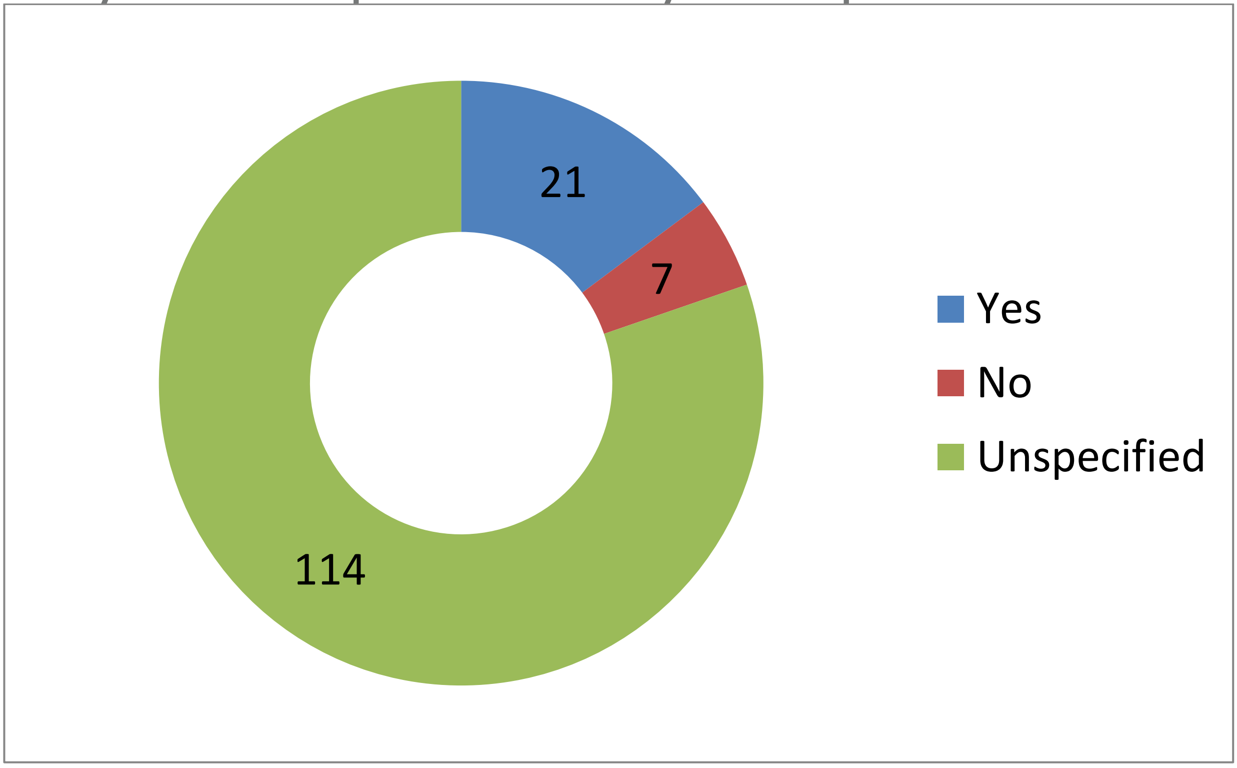
Who carries out load testing?



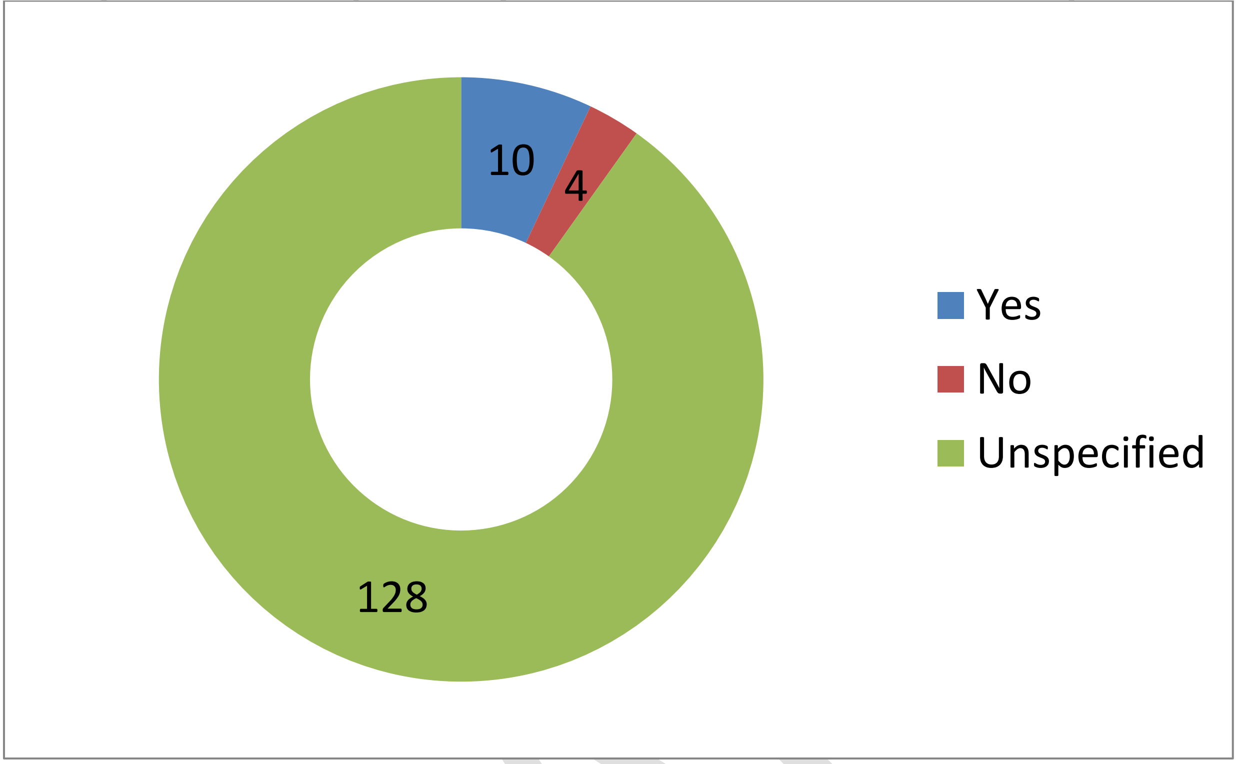
Who carries out unit tests?



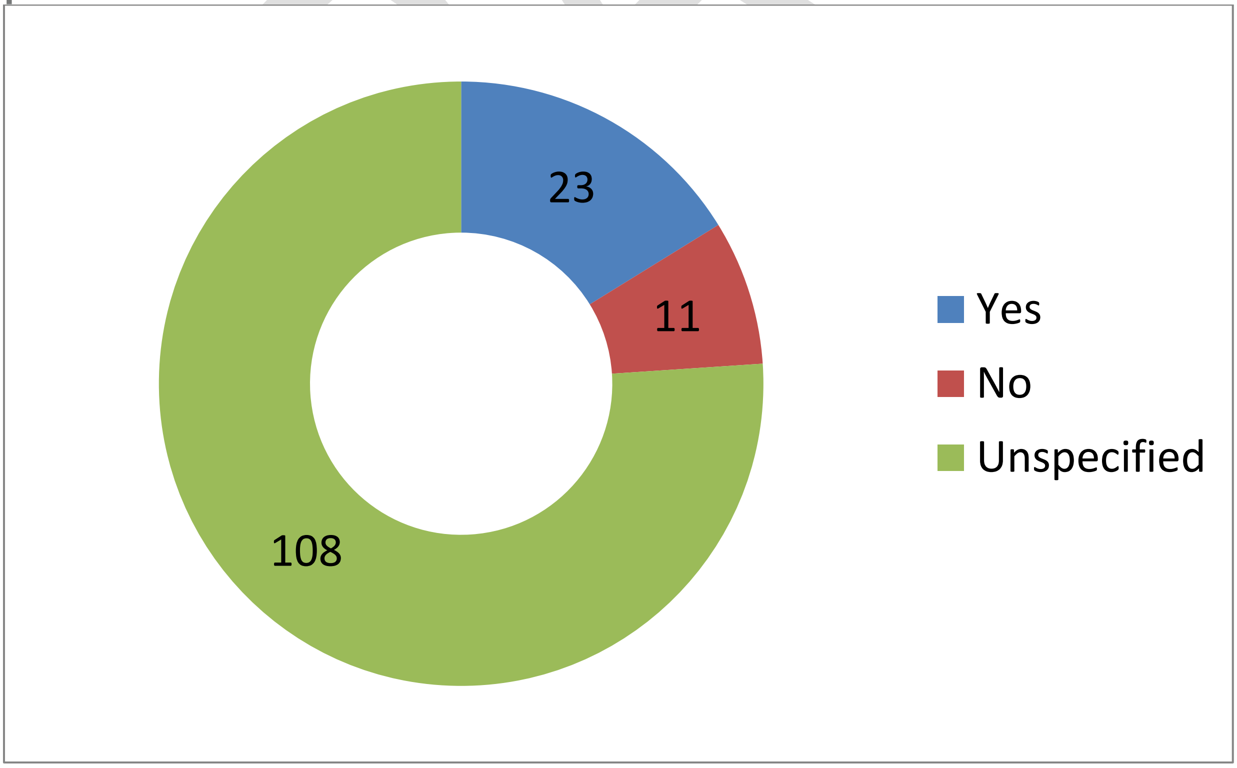
Have you received reports on availability from the provider?



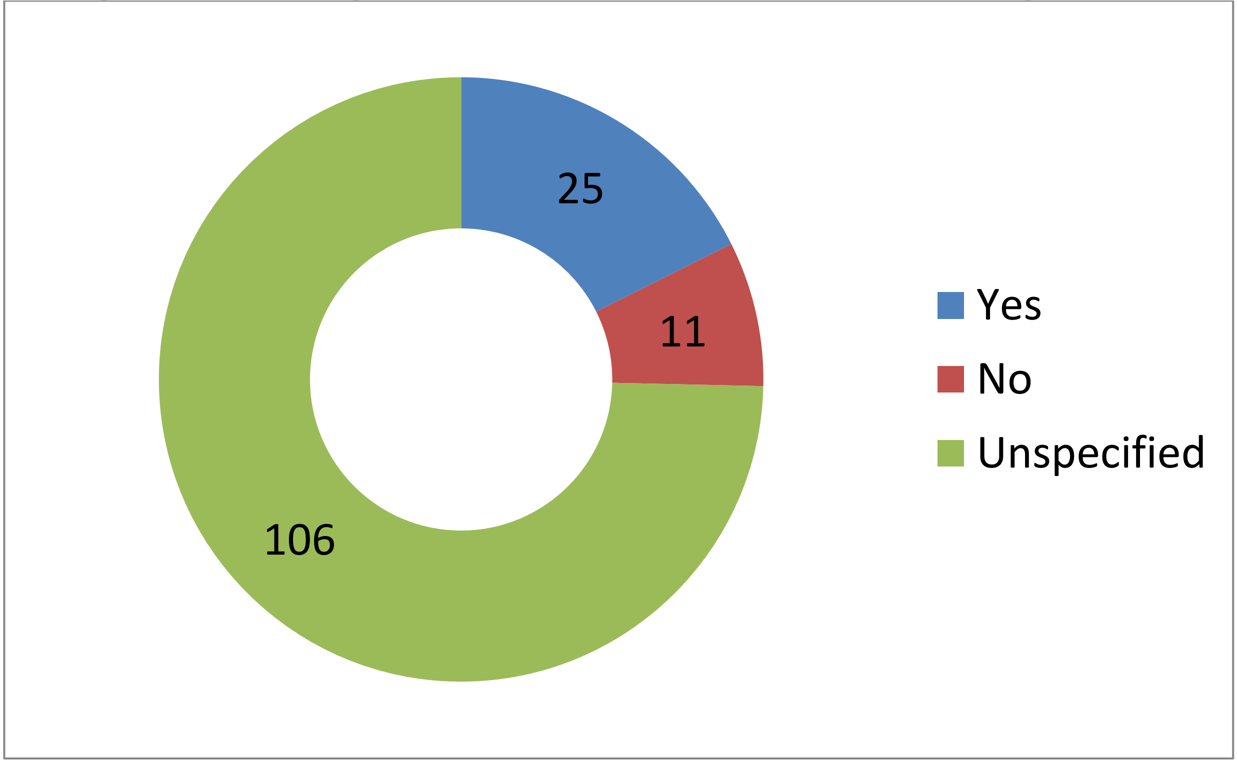
Have you received reports on penetration tests results from the provider?



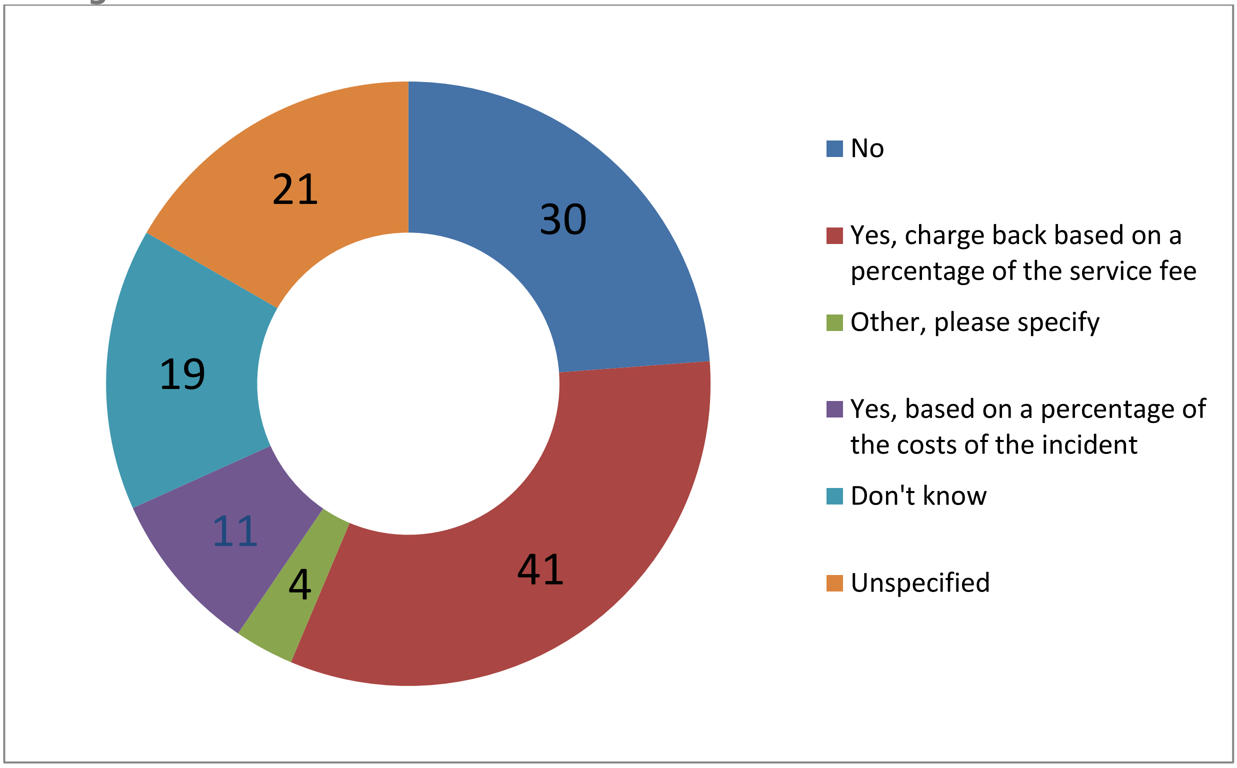
Have you received reports on failover and backup tests from the provider?



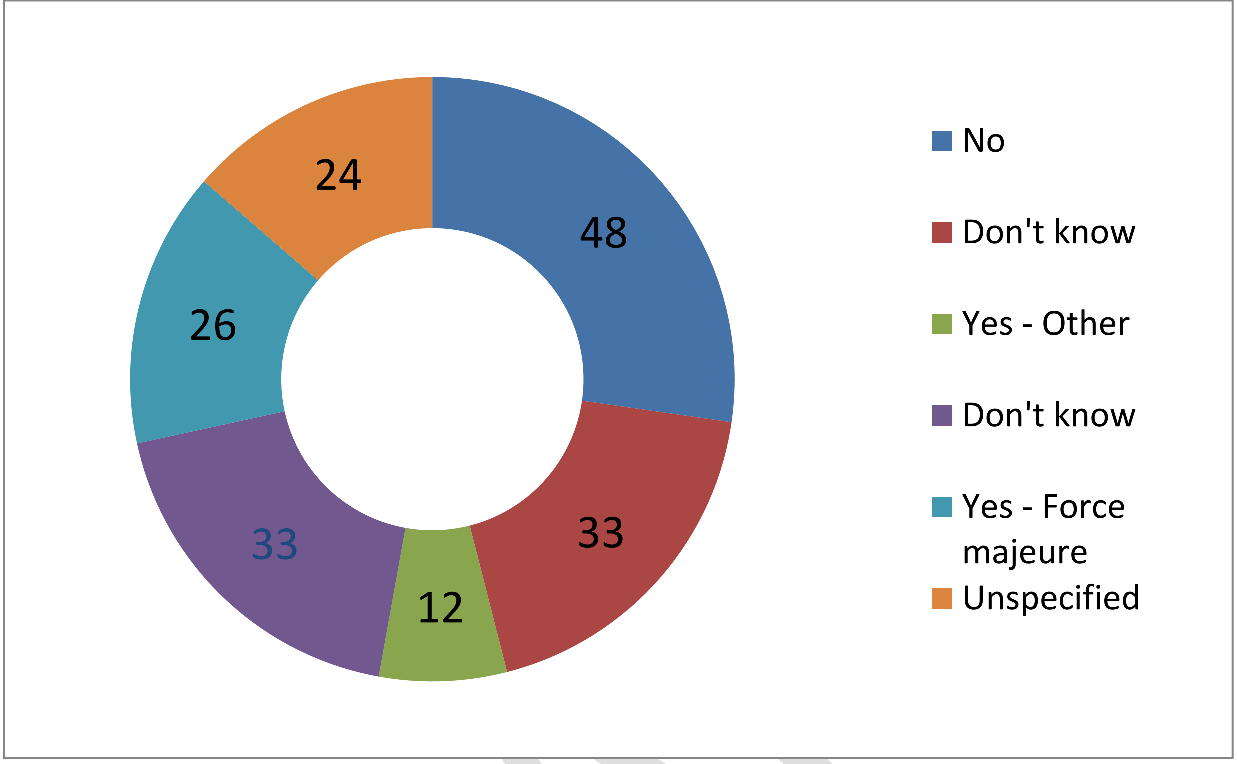
Have you received reports on failover and unit tests from the provider?



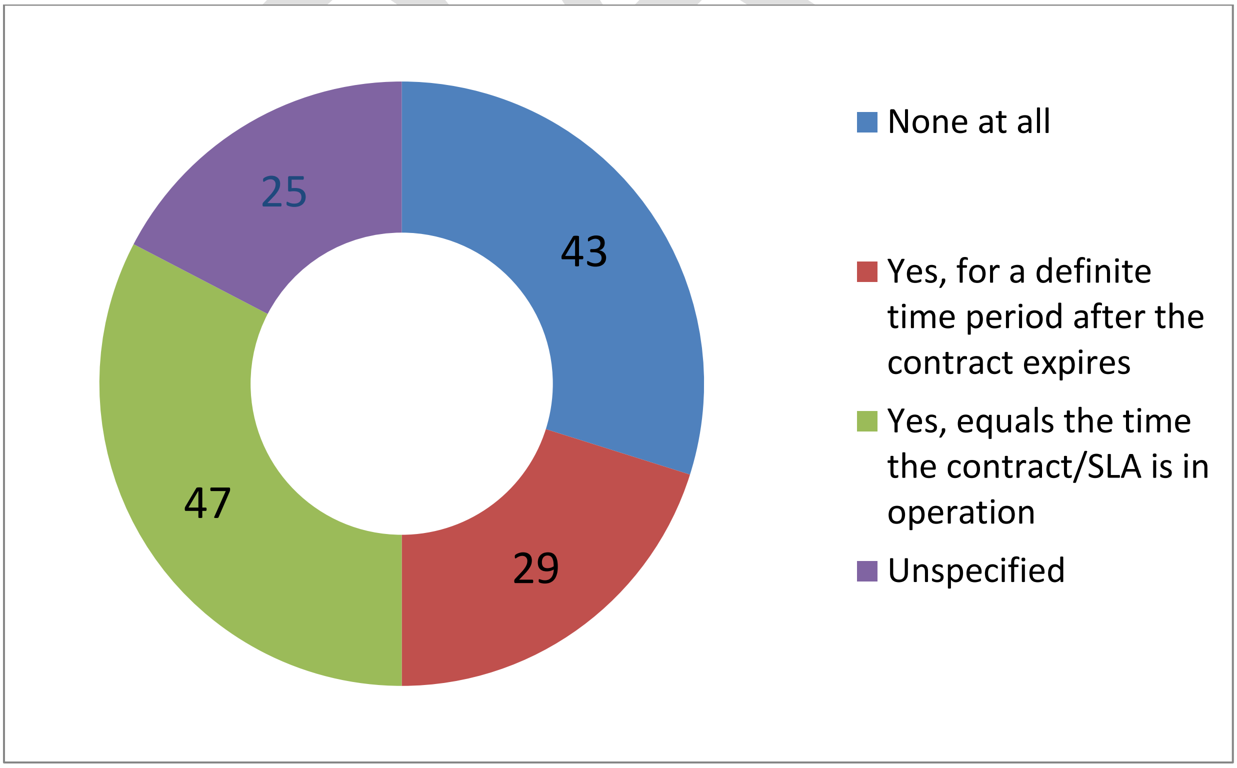
Does the SLA define penalties when the service provider does not meet the agreed service levels?



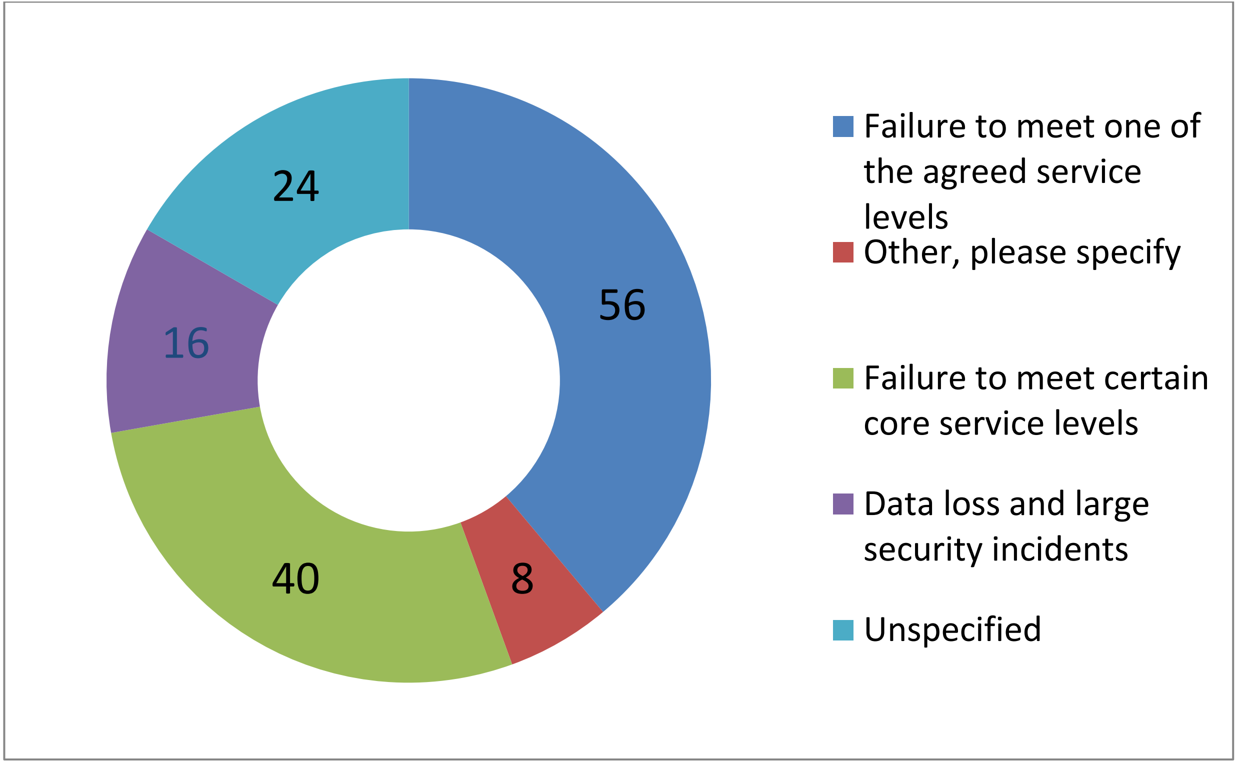
Are there penalty exclusions?



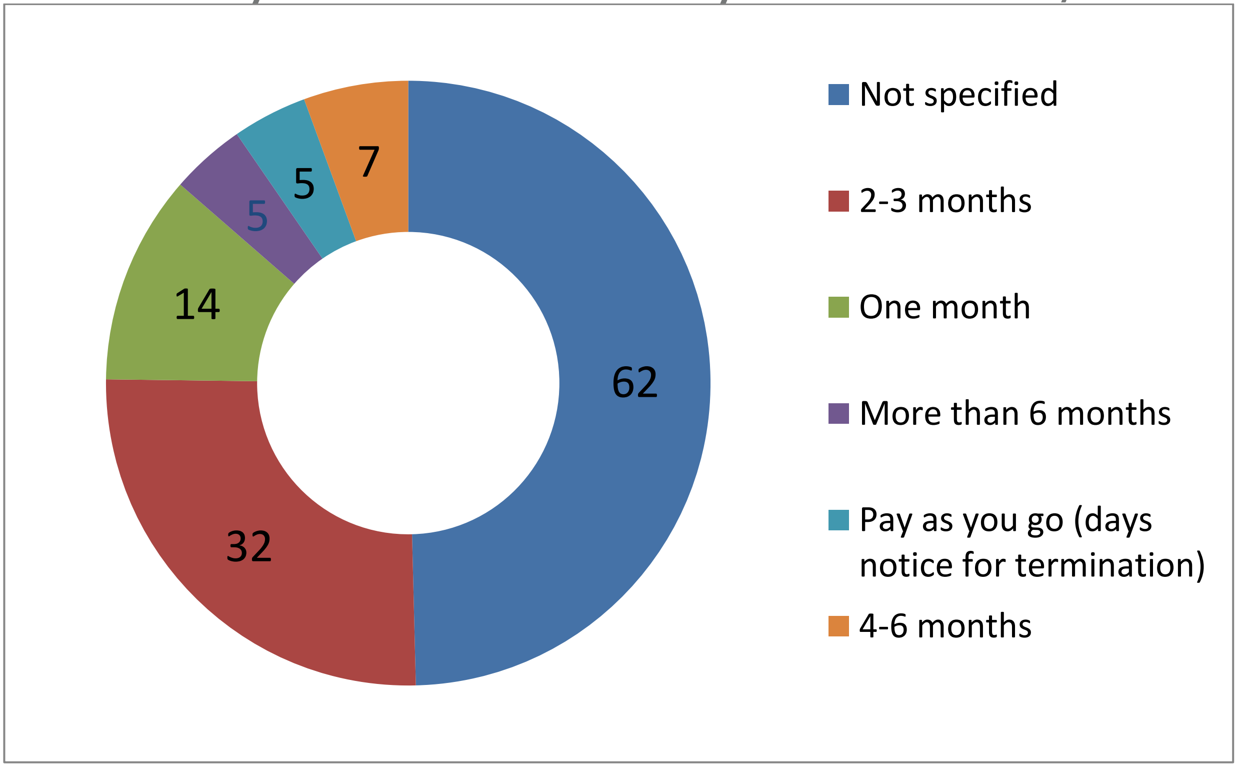
Do you have requirements in your contract/SLA on how long data must be retained and available?



When is the SLA/contract considered breached?



After how many months of SLA breach can you exit the contract/SLA?



ENISA – European Network and Information Security Agency
PO Box 1309, 71001 Heraklion, Greece
Tel: +30 2810 391 280
Fax: +30 2810 391 410

www.enisa.europa.eu