enisa
European Network
and Information
Security Agency

Survey and analysis of security parameters in cloud SLAs across the European public sector

[Deliverable 2011-12-19]

About ENISA

The European Network and Information Security Agency (ENISA) is a centre of network and information security expertise for the EU, its member states, the private sector and Europe's citizens. ENISA works with these groups to develop advice and recommendations on good practice in information security. It assists EU member states in implementing relevant EU legislation and works to improve the resilience of Europe's critical information infrastructure and networks. ENISA seeks to enhance existing expertise in EU member states by supporting the development of cross-border communities committed to improving network and information security throughout the EU. More information about ENISA and its work can be found at www.enisa.europa.eu.

Contact details

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

- Dr Marnix Dekker, Dr Giles Hogben
- Internet: http://www.enisa.europa.eu

For questions related to the survey please use the following details:

- E-mail: resilience@enisa.europa.eu

The survey data in this document was collected by IDC under contract with ENISA

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 a legal 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 information purposes only. It must be accessible free of charge. 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.

Reproduction is authorised provided the source is acknowledged.

Contents

Executive summary

In the past, organizations would buy IT equipment (hardware or software) and manage it themselves. Today many organizations prefer to use cloud computing and outsourced IT services. The work of an organisation's IT officer has changed as a consequence: Instead of setting up hardware or installing software, IT officers now have to manage IT service contracts with vendors (cloud, datacentre, infrastructure, etc..). This survey gives a snapshot of how the IT officers in the European public sector are currently managing the security aspects of these service contracts. The survey produced full responses from 117 IT officers, from 15 different EU countries and all layers of government, who are either involved in procuring cloud or IT services or responsible for managing the SLAs.

Take for example a customer who procures a set of enterprise servers from a service provider. In the RFP phase the customer would request for a patching and hardening process to be in place. In this phase, security control frameworks play an important role, for example the ENISA assurance framework, the ISO27001 or the CSA Cloud Control Matrix. These frameworks, however, are used for a one-time, or yearly assessment of the security measures in place.

Therefore the customer should define security requirements via parameters in the SLA which can be continuously monitored (the maximum time to patch e.g.) and agree with the service provider to receive sufficient monitoring data (such as results from vulnerability scans or incident reports after failed patching). Without definitions and provisions about security parameters and security monitoring, it is hard for the customer to evaluate security and to know if the service provider delivers accordingly to the (security) requirements.

This document focuses on what is measurable in the contract: the Service Level Agreement (SLA) and how continuous monitoring is implemented. If a customer wants to be able to monitor the security of a service then it is important that the SLA contains measurable definitions of security parameters and that the customer receives reports about measurements and incidents.

We asked respondents to reply to our survey for only one service contract. As mentioned, we obtained 117 fully completed responses from IT officers across the European public sector (in 15 different EU countries). Most respondents (77%) said there are high or very high security requirements (41% and 36%) for the service in question (replying 4, and 5 on a scale from 1 to 5). Security is clearly a top concern for most respondents. But our survey also shows that many customers do not monitor security aspects on a continuous basis.

The survey data shows that while SLAs are often used, and availability is often addressed in these SLAs, other security parameters are less well covered. Availability is often defined in contracts or SLAs and also monitored on a regular basis:

- 75% of the contracts define availability requirements.
- 50% of the contracts stipulate that availability be measured regularly.
- In 78% of the cases the provider is obliged to report service outages.

Other security parameters are less well covered.

- Only 32% of contracts include a classification of security incidents.
- In 57% of the cases penetration tests have been performed at some point, but only in 16% of the case penetration tests were performed regularly.
- Data portability is tested regularly in only 12% of the cases.
- Only 50% require load testing after first use
- Failover and backup tests are carried out regularly only in 26% of the cases.

Even if parameters are covered in contracts, customers do not always receive regular service level reports. For example, the survey shows:

- Only 15% received availability reports
- Only 7% receive penetration test reports
- Only 16% receive failover and backup reports.

Finally, although it may not apply in all settings, it is notable that service levels are linked to penalties only in 44% of cases.

By publishing the results of this survey we draw attention to the fact that many customers do not monitor security measures continuously. This means that customers are in the dark about many important security aspects of their services. The risk is that they find out about failing security measures when it is already too late.

Survey analysis

In this section we analyse the survey results and provide some pointers to best practice in setting up and monitoring SLAs. Apart from certification and assurance frameworks, such as ISO 27001 and cloud-focused frameworks such as the ENISA Assurance Framework and the CSA controls matrix, an important part of managing contracts is the specification, monitoring and verification of security parameters via an SLA. For example, in an SLA the customer and the provider agree on technical details like daily backups, weekly patching, 99% uptime, one hour recovery time objective, etc. The customer should ensure that these service levels can be and are monitored by the customer or by the provider or some third party and that the customer is provided with monitoring data. It makes no sense to require 'availability' of a certain service if there is no clear definition of this term, nor any agreement on how this should be monitored.

Regardless of the parameters are relevant in a given service context, the following list issues are important to take into account:

1. **Parameter definition:** a definition of exactly what is being measured. For example, not just availability, but a detailed definition of what availability means in terms of basic functions, their expected operation (how long to send an email e.g.).
2. **Monitoring methodology:** The methodology for measuring real-time security parameters should be clearly understood before the contract is established. This includes techniques for obtaining objective measurements, sub-indicators, etc... For example, for availability, a technique might be the use of active probes. A sub-indicator might be the number of customer calls about availability issues.
3. **Independent testing:** Wherever feasible technically and economically, independent testing of the SLA parameters should be carried out. Some monitoring may be easily and economically carried out by the customer themselves, while others can only be run on a system-wide basis by the service provider and cannot be carried out by a single customer (or are too expensive). Examples of parameters which can be tested independently include availability, business continuity.
4. **Incident/alerting thresholds:** Contracting parties should define the ranges of parameters that trigger ad-hoc alerts, incident response or remediation. For example, for resource provisioning, a typical trigger point would be the inability to provision extra resources of more than 10% of existing resources per day.
5. **Regular reporting:** Regular Service Level Reports (SLRs) and their contents should be defined. SLRs typically include for example, incidents, event logs and change reports.
6. **Risk profile considerations:** response thresholds should be determined according to the risk profile of an organisation. For example, a low-cost service for batch-processing non-personal data does not need high levels for confidentiality requirements. SLA's and in particular incident reporting, alerting and penalty triggers should be adapted to an organisation's risk-profile.
7. **Penalties and enforcement:** depending on the setting, parameter thresholds can be linked to financial penalties, to incentivize compliance with contractual requirements or compensate for certain losses.

As a follow-up, ENISA will publish a detailed best practice document, based on consultation with a stakeholder group, including some of the respondents to this survey. This will analyze in detail, the parameter breakdown (1-7 above) for a number of parameters, such as availability, elasticity, data backup, data portability, isolation, access control, incident response and recovery, patching, vulnerability detection and intrusion prevention.

In this document, we have included, where applicable, guidance notes to best practice in each question area (some areas, such as the country of the respondent do not have any associated best practice). The following summarises the most important points addressed:

General points

- If service providers do not comply with the same minimum standards (not necessarily the same governance framework), as the customer, this undermines the value of the overall information security management processes. Governance and certification frameworks of a similar assurance level should be applied across the supply chain.
- Best practice is to involve security experts in the contract setup phase, to review and validate the contract against security objectives.

Availability

- It is very important to define availability criteria clearly, including the number of affected users, service scope and the criteria for service uptime. Failure to do so reduces the value of availability clauses in case of an incident.
- Availability should be tested and reported frequently, preferably independently by the customer and the provider.
- Availability and uptime requirements should be increased according to the degree to which it is critical that a service is:
  - Available at a given point in time (for example real-time market analysis would require high availability). In this case the SLR would focus on MTTR – mean time to recovery.
  - Available for a given percentage of total operational time (for example, for a data analysis service).
  - Not replicated either by the service provider or available from another source.
- The reporting window for availability depends on the type of service. Services with high requirements for real-time response should apply shorter term reporting windows for availability.
- Scalability and elasticity requirements should be included in an SLA particularly for contracts where a high demand volatility is anticipated.

Incident response

- Classification of security incidents in reports from the service provider helps to manage appropriate response. It also helps to comply with any regulatory requirements for breach or incident reporting.
- The timely reporting of incidents is critical to limit their impact (e.g. by revoking compromised credentials, informing affected customers, etc…)

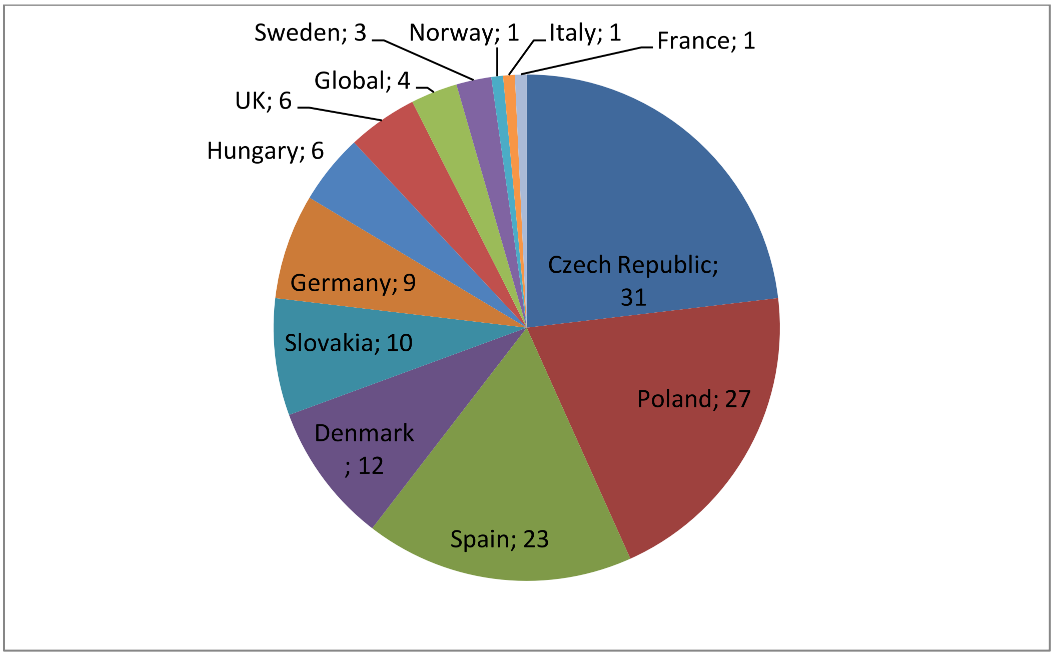
Testing

- Penetration tests should be carried out frequently and preferably independently by the customer and the provider.
- For penetration testing, customers may need permission to run penetration tests – the conditions for performing penetration tests may be established contractually.
- Unit testing (automated testing of system components with well-defined exit-criteria) ensures not only availability of network response, but the actual functioning of services according to the contract requirements. It can also test for vulnerabilities on a continuous basis.
- For services with highly volatile demand, it is especially important to test the load tolerance of the system.
- Testing of data portability can be critical to business continuity in the event of a provider failure or bankruptcy.
- In all tests, it is preferable, where technically and economically feasible that either the customer or an independent organisation carries out the tests (as well as the service provider).

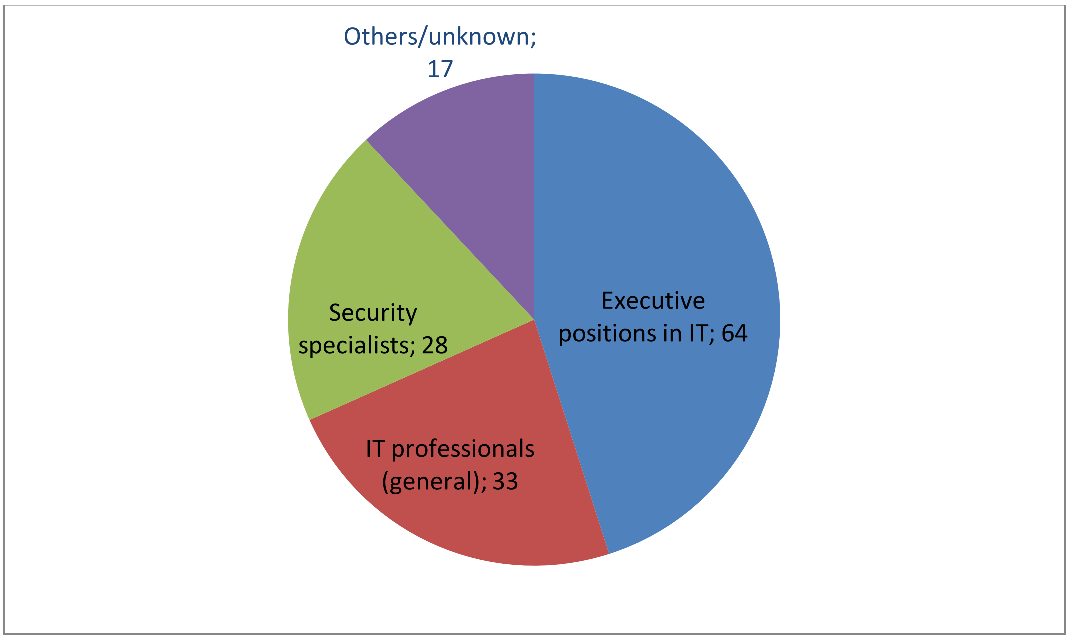
Survey results

In this section we provide the statistical results from the survey. The raw response set (as a spreadsheet), containing only anonymized data, can be provided on request (see colophon).

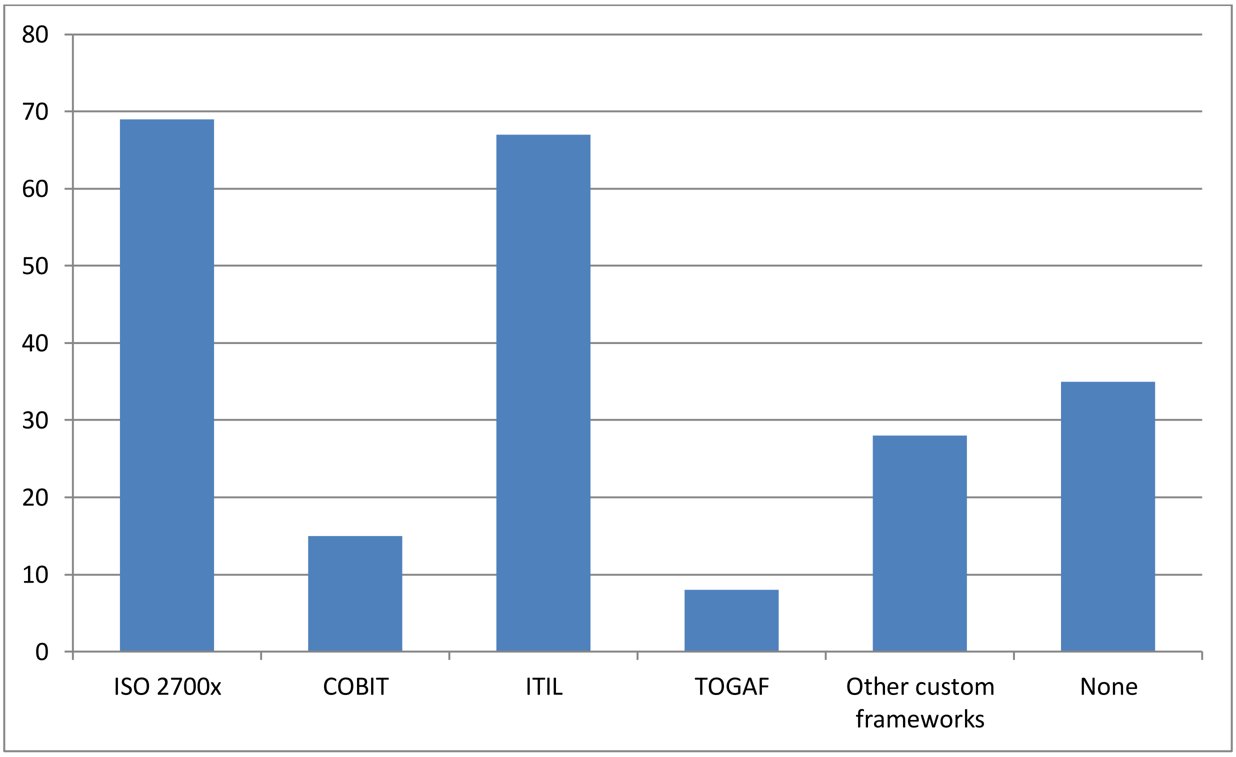
1.1 Number of respondents per country



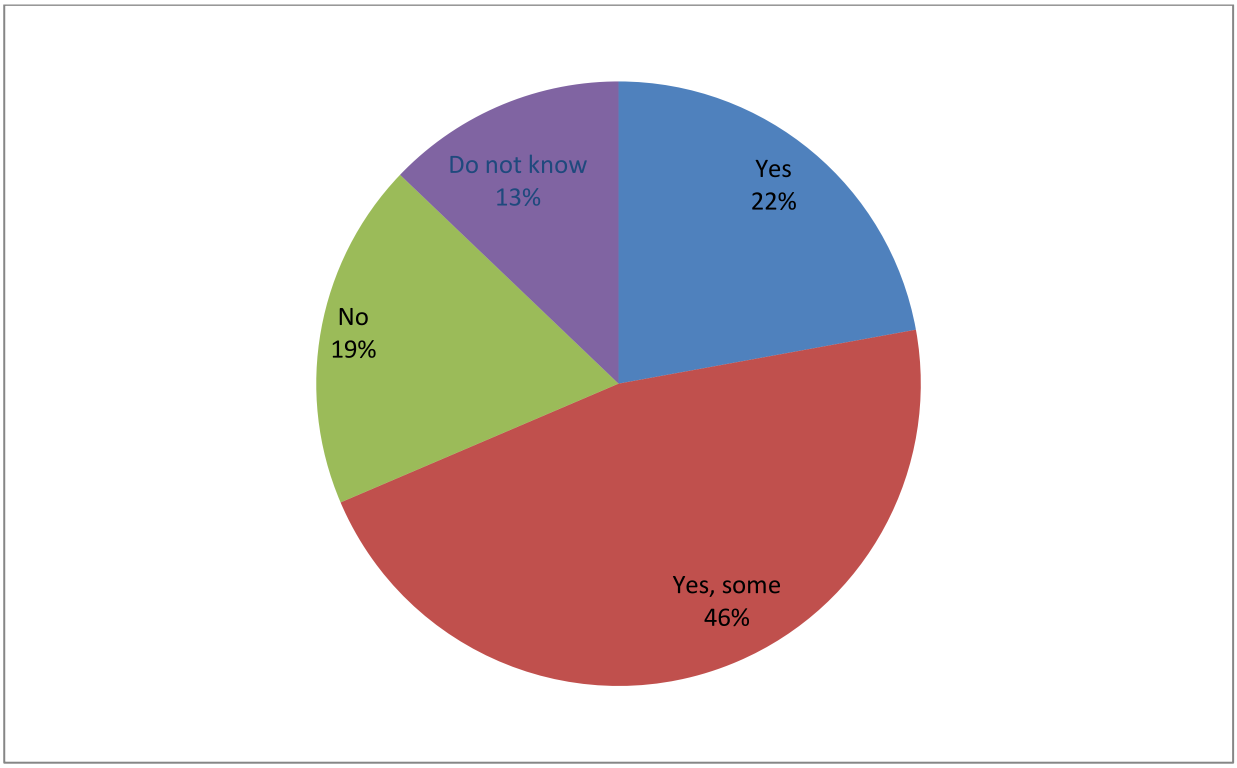
1.2 Role of the respondent



1.3 Governance frameworks and security standards used (number of respondents)

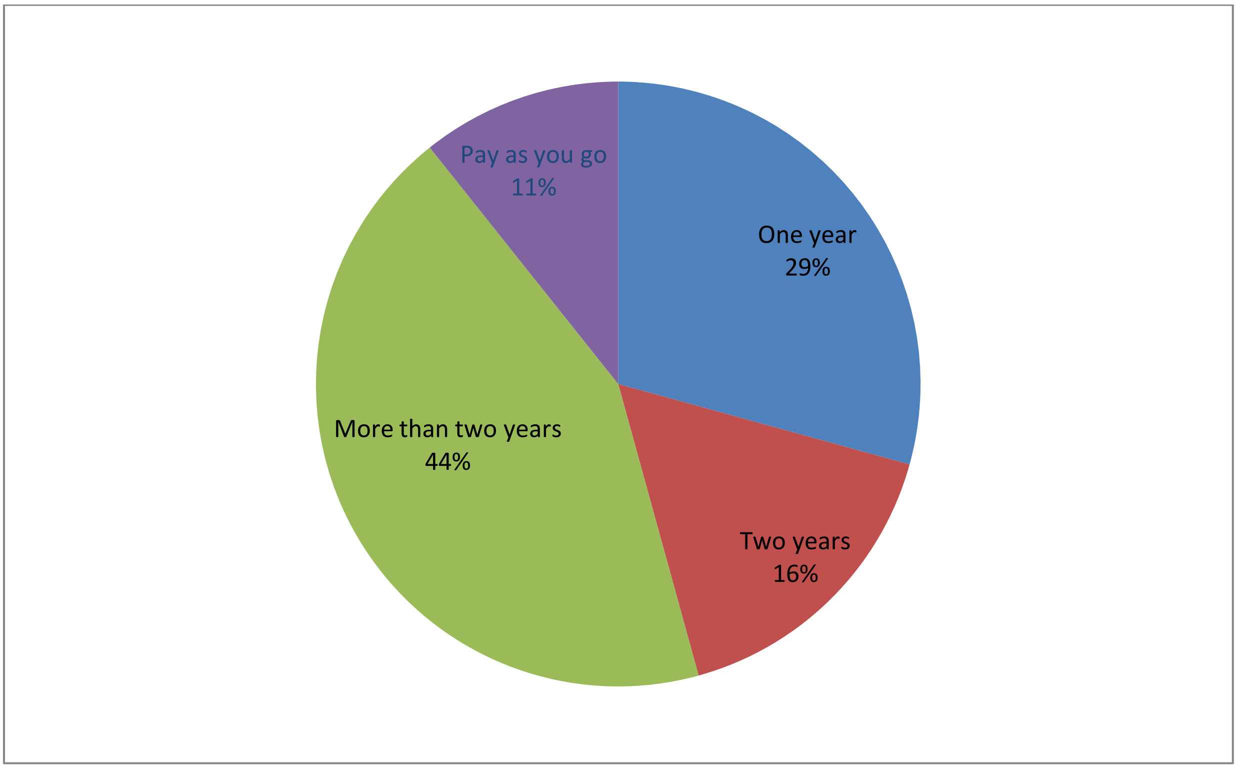


1.4 Are your IT service providers obliged to adhere to these standards too?

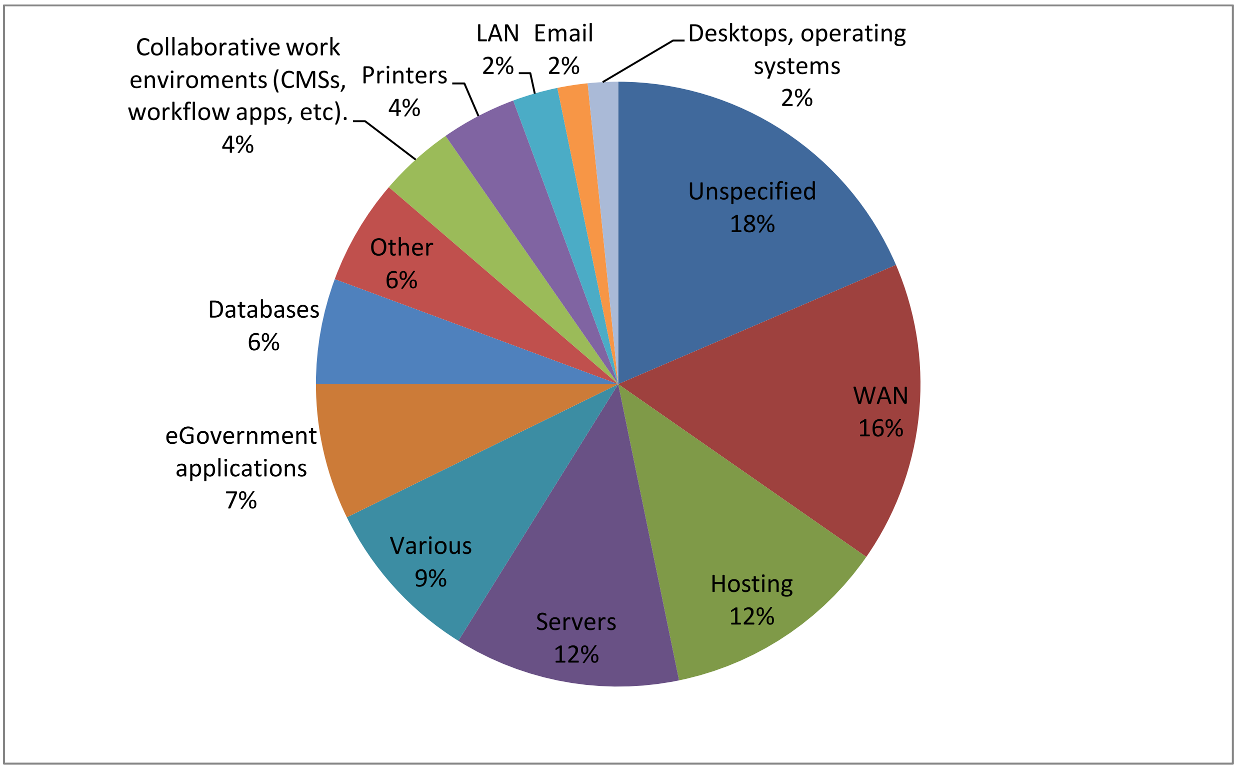


Notes: if service providers do not comply to the same minimum standards (not necessarily the same governance framework), as the customer, this undermines the value of the overall ISMS.

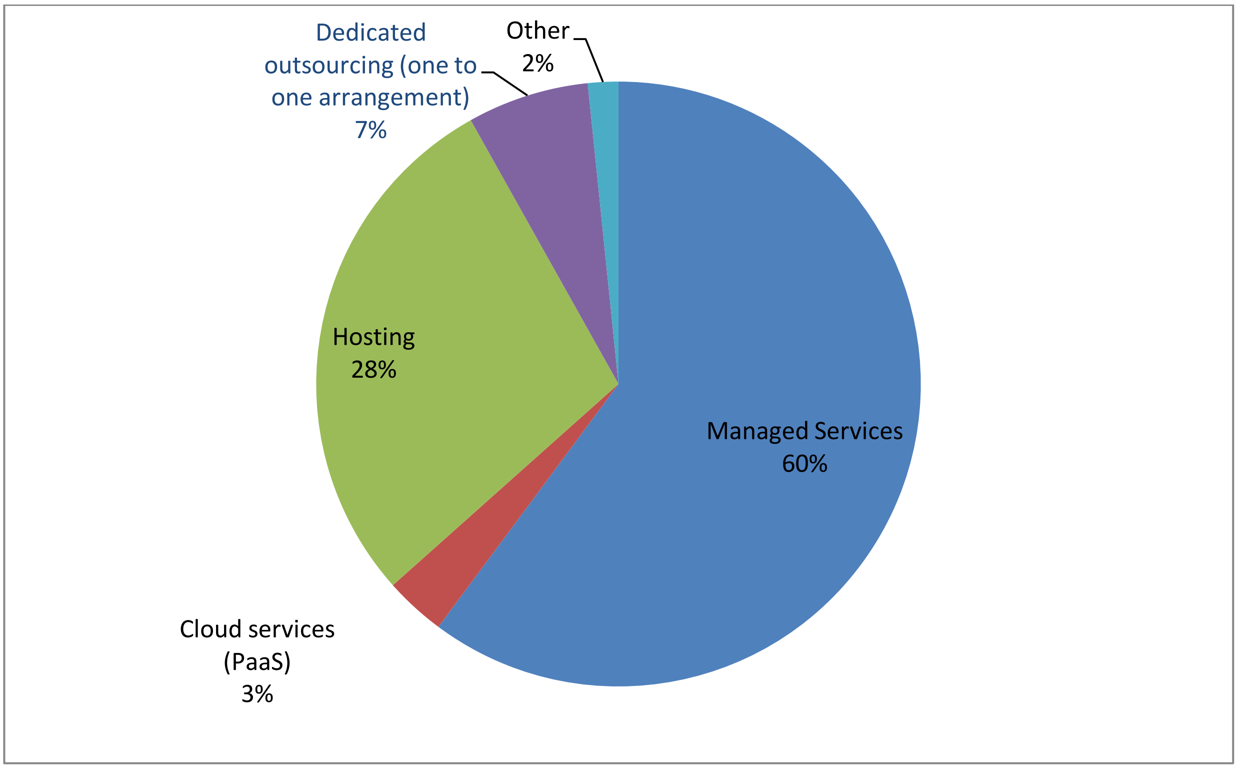
1.5 How long does the contract/SLA last?



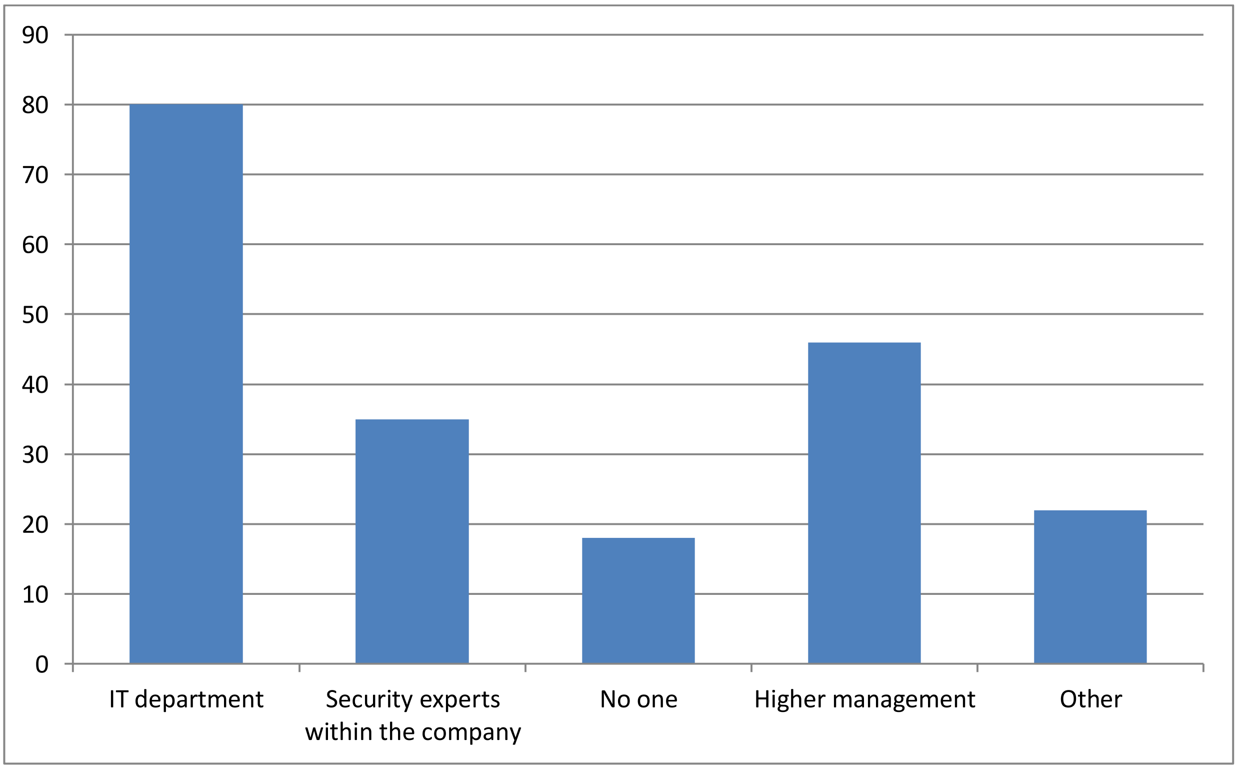
1.6 Types of infrastructure or applications covered by the SLA/contract



1.7 Types of the contracts/SLAs

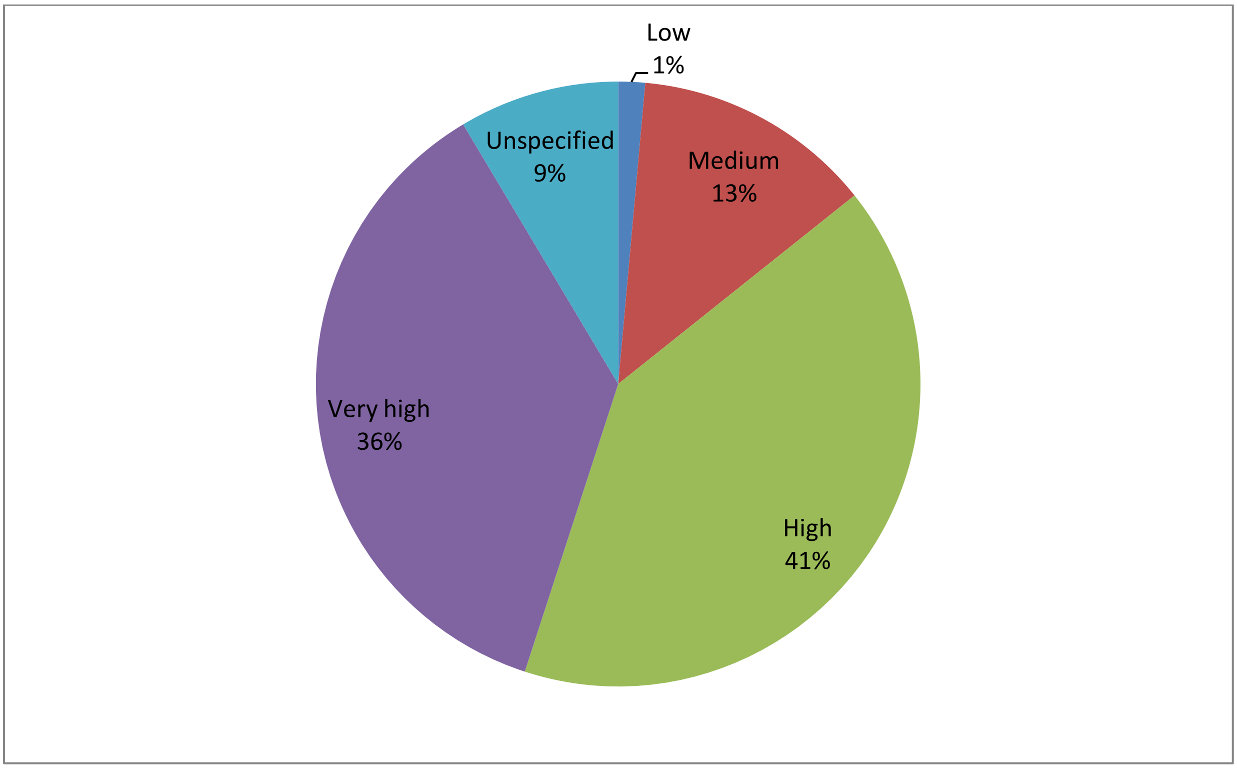


1.8 Who was involved in setting the SLA/contract?



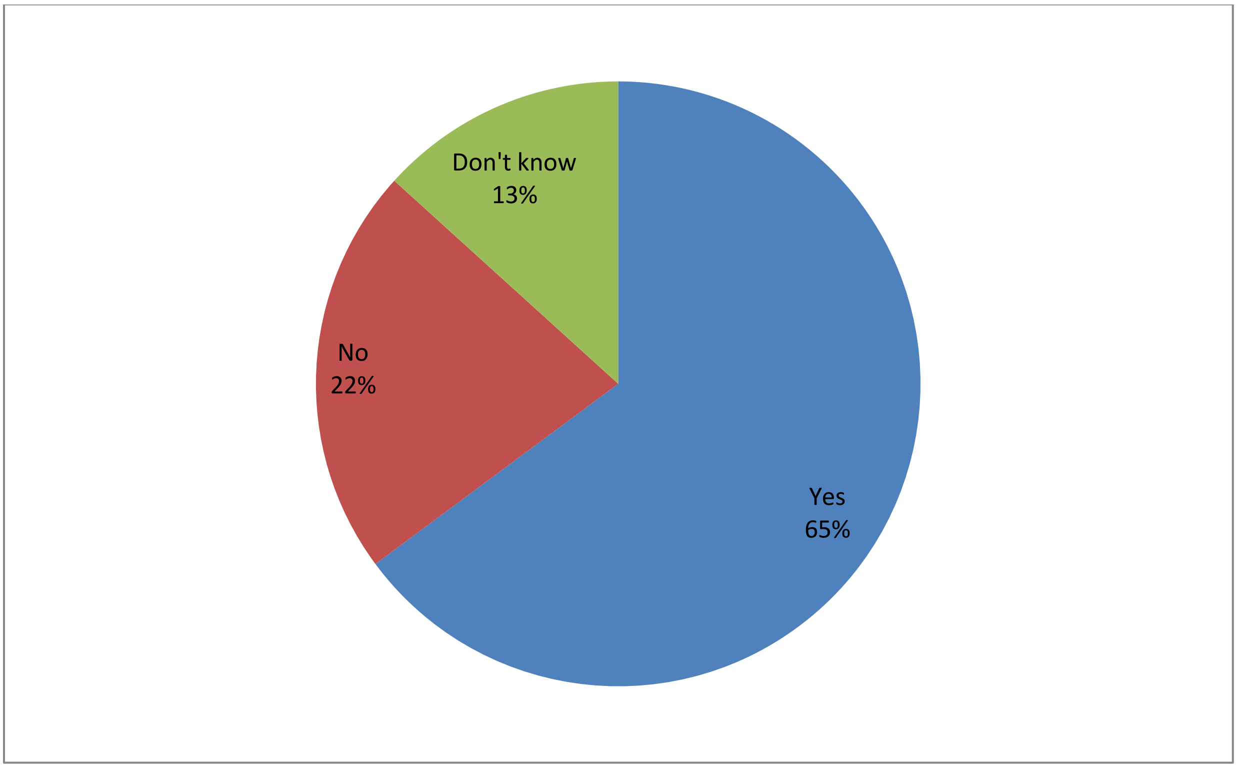
Note: best practice is to involve security experts and at minimum the IT department in order to validate security-related requirements.

1.9 Security requirements rating



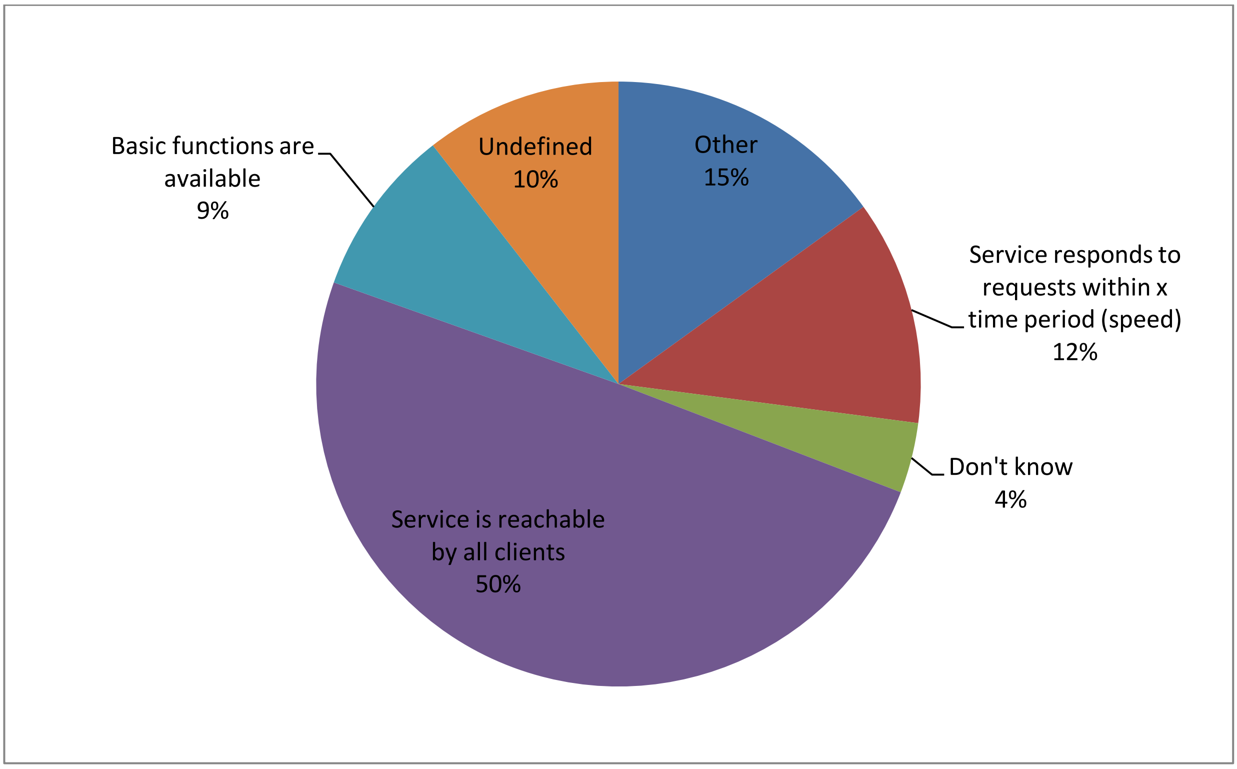
Note: public sector projects generally have high security requirements.

1.10 SLA defined



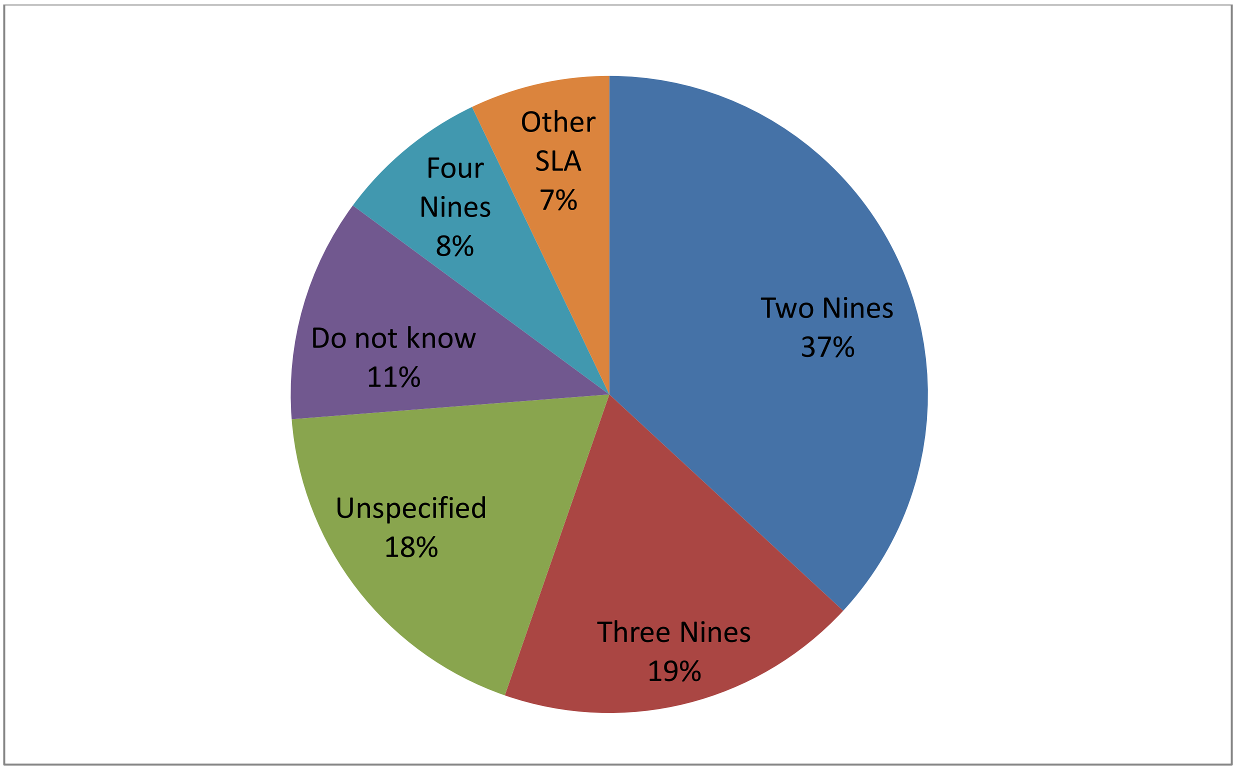
Note: the definition of an SLA is an important prerequisite for ensuring security within an outsourced project.

1.11 Define availability



Note: it is very important to define availability clearly, including the number of affected users, service scope and the criteria for when a service is considered to be available.

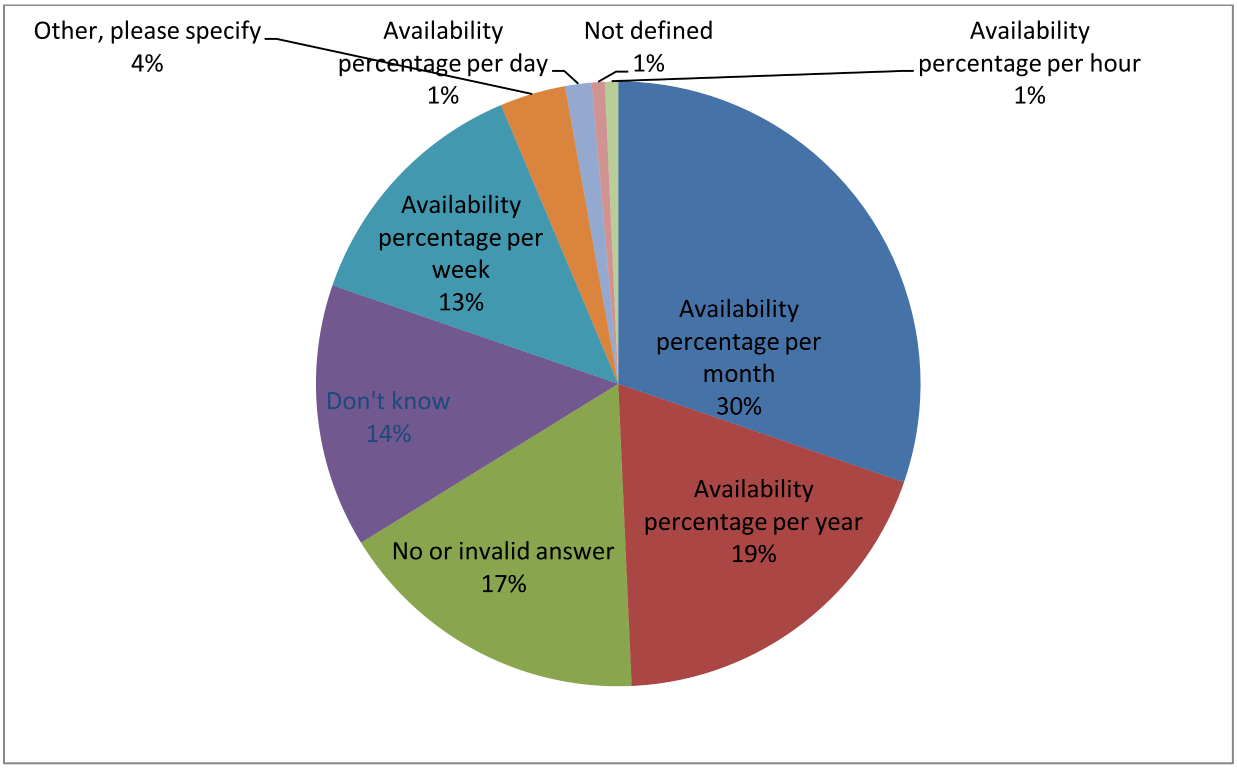
1.12 Availability requirements



Note: Availability requirements should be modified according to the degree to which it is critical that a service is:

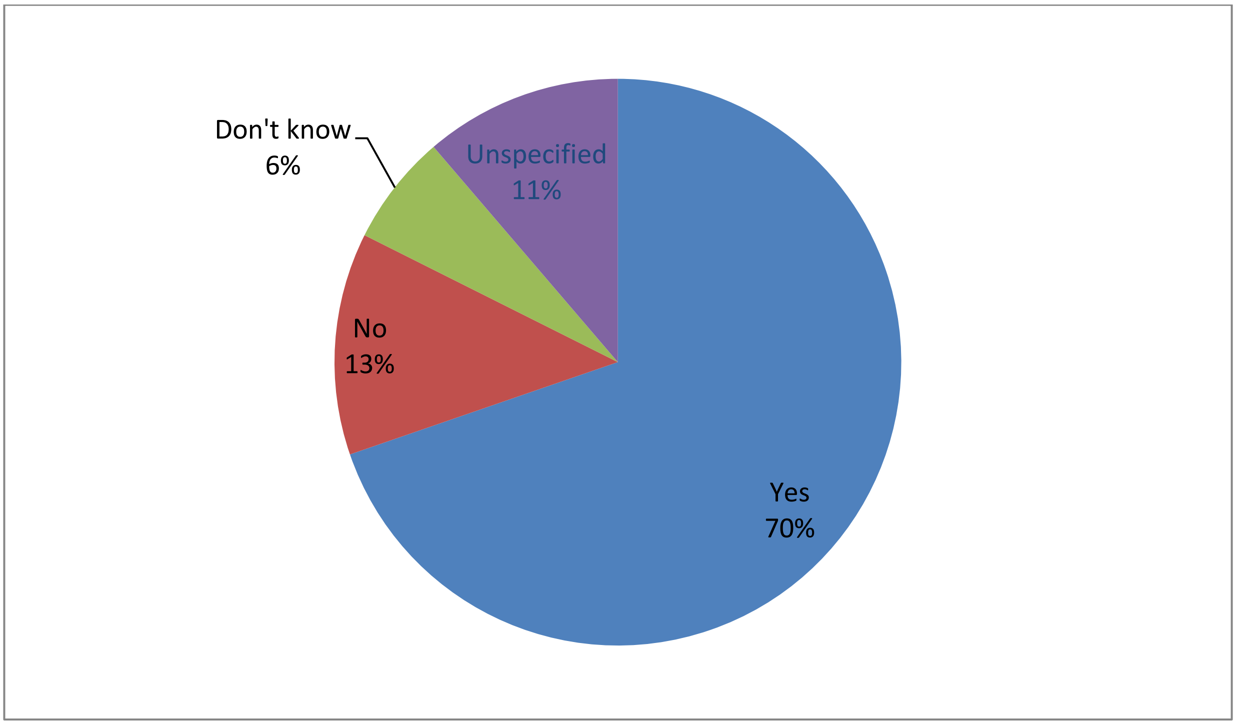
- Available at a given point in time (for example real-time market analysis would require high availability). In this case, the MTTR (Mean Time to Recovery) is also an important parameter.
- Available for a given percentage of time (for example, for a data analysis service).
- Not replicated either by the service provider or available from another source.

1.13 Availability definition period



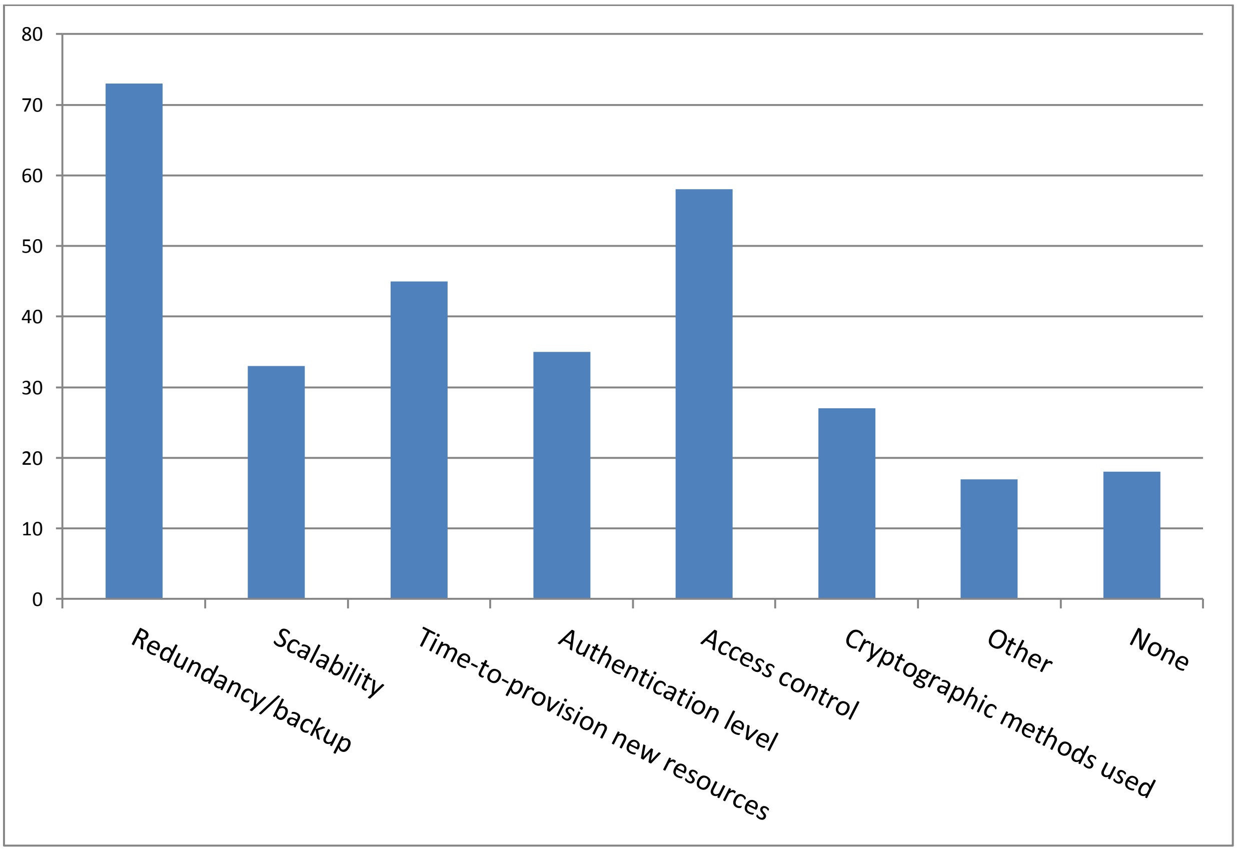
Note: the reporting window depends on the type of service. Services with high requirements for real-time response should apply shorter term reporting windows for availability.

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



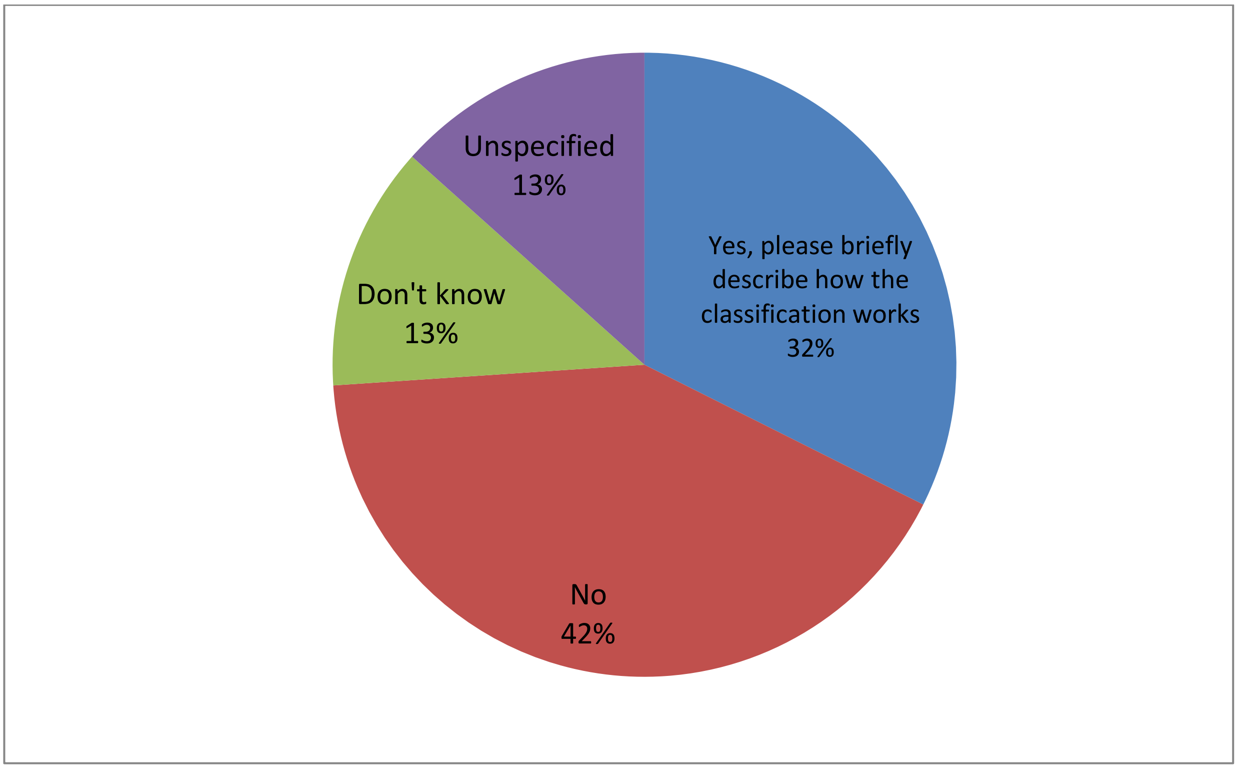
Note: reporting times for downtime should be subject to a time limit.

1.15 Which of the following aspects did you explicitly address in your SLA/contract? (number of respondents)



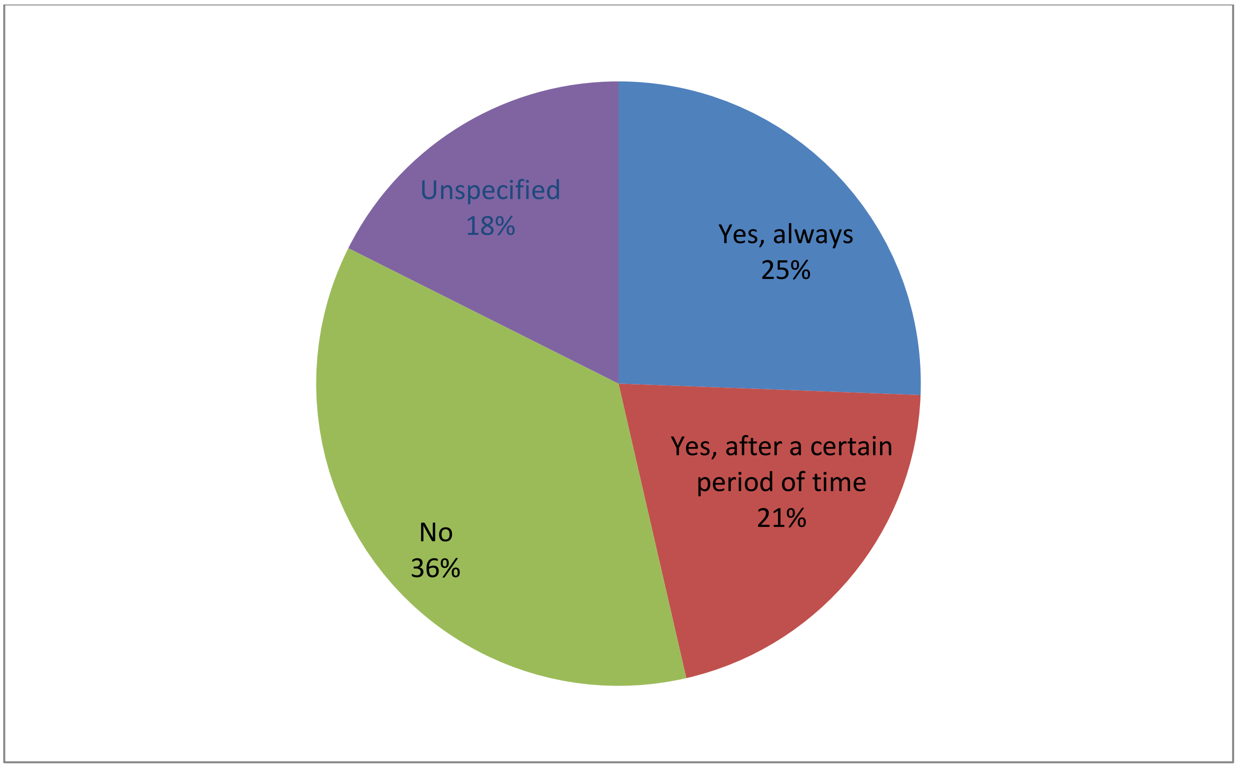
Note: scalability is important to address specifically for cloud service providers as this is one of the major business advantages offered by cloud computing.

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

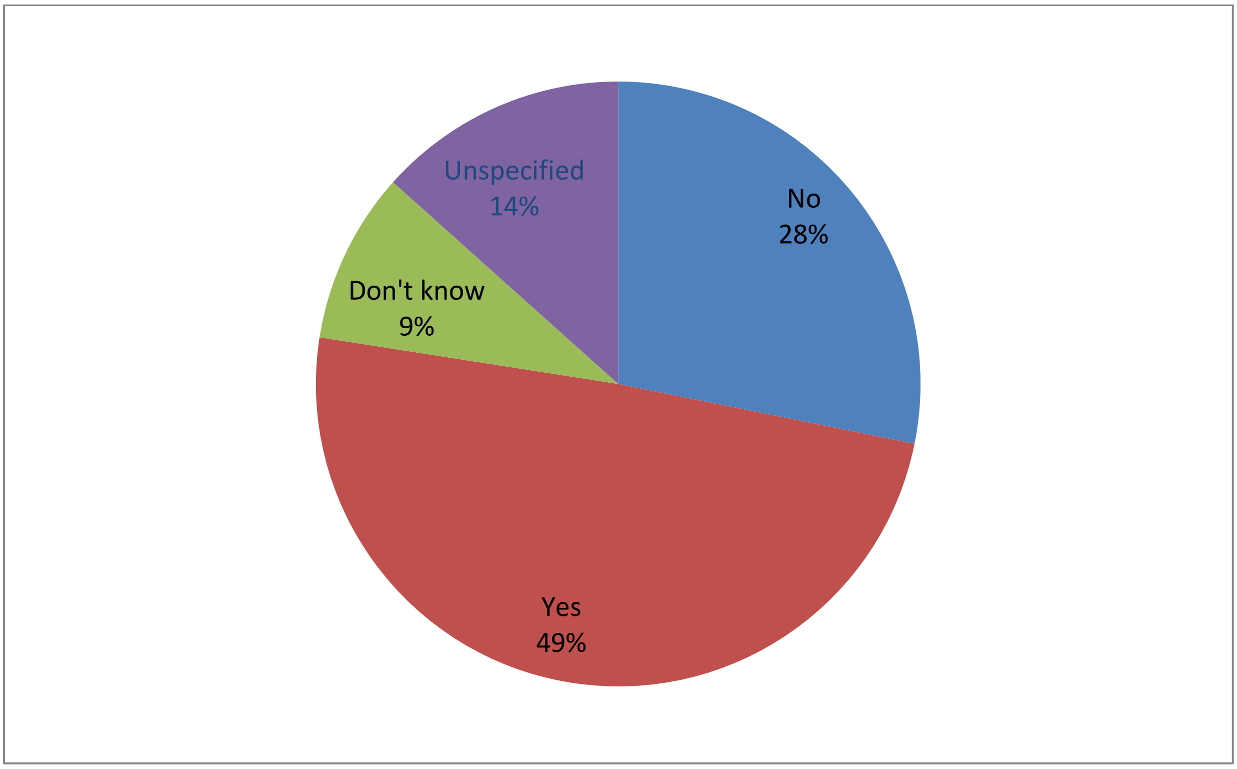


Note: classification of security incidents helps to manage appropriate response. It also helps to comply with any regulatory requirements for breach or incident reporting.

1.17 The definition of security incidents includes secondary system incidents?

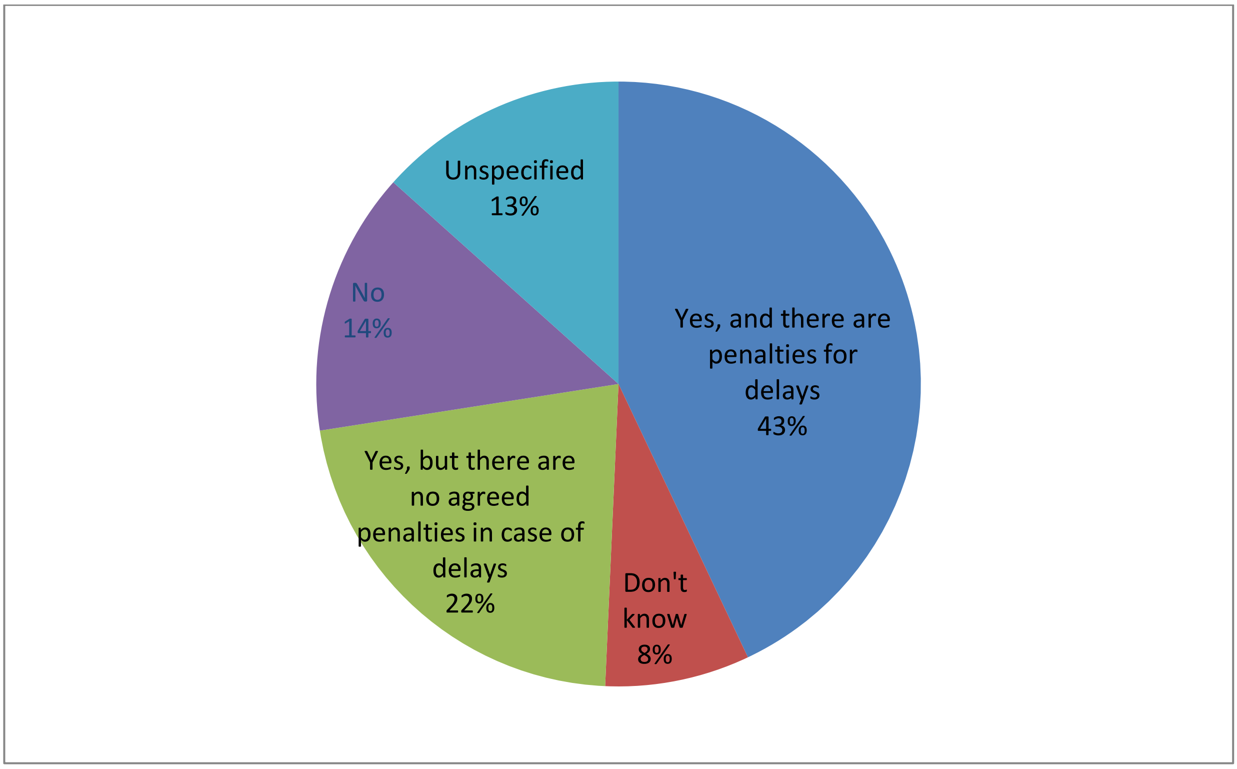


1.18 Does the SLA/contract oblige the service provider to report security incidents, within a certain time frame?



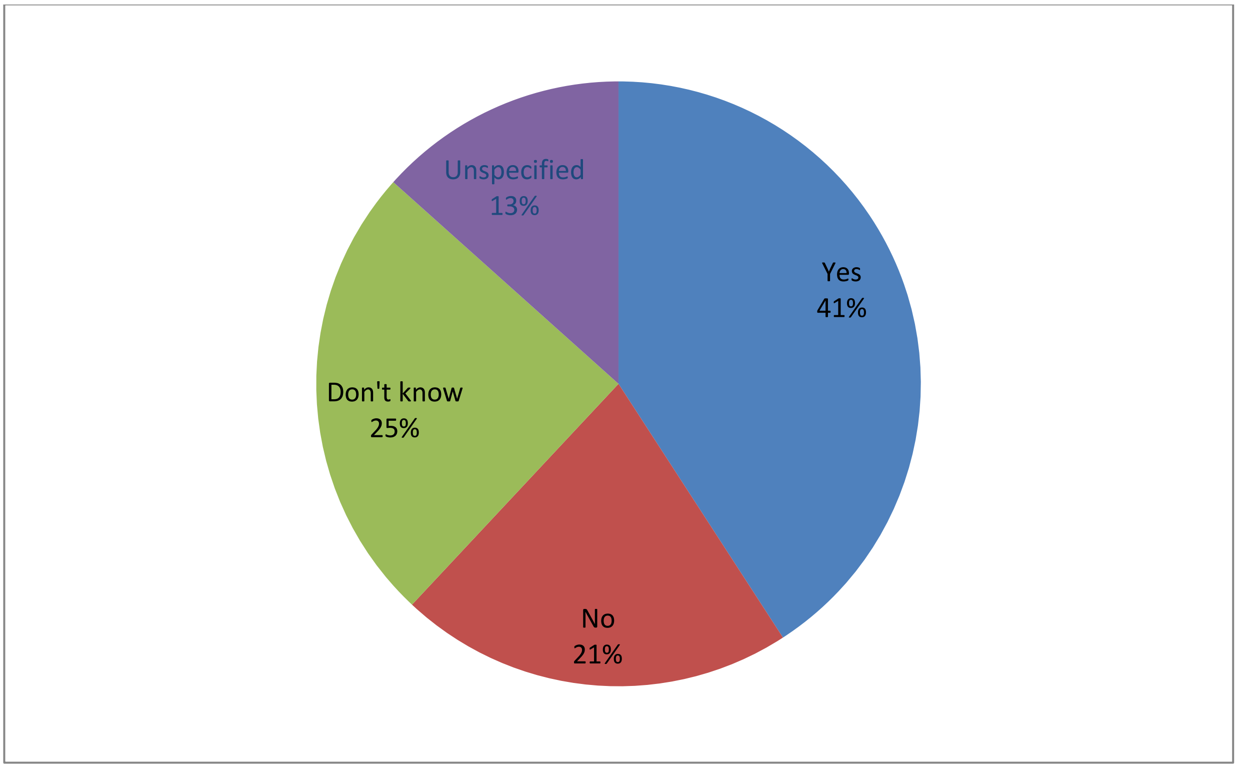
Note: the timely reporting of incidents is critical to limit their impact (e.g. by revoking compromised credentials, informing affected customers, etc…)

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

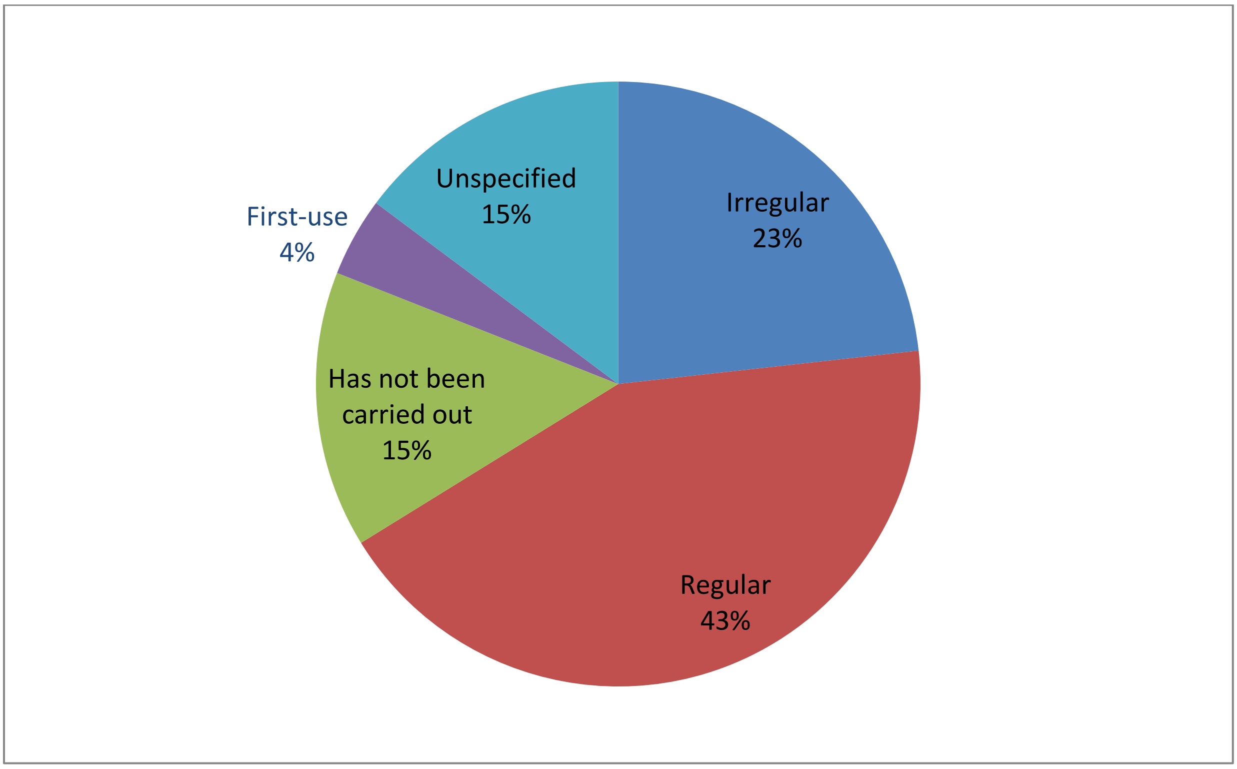


Note: Recovery time objective should be minimized.

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

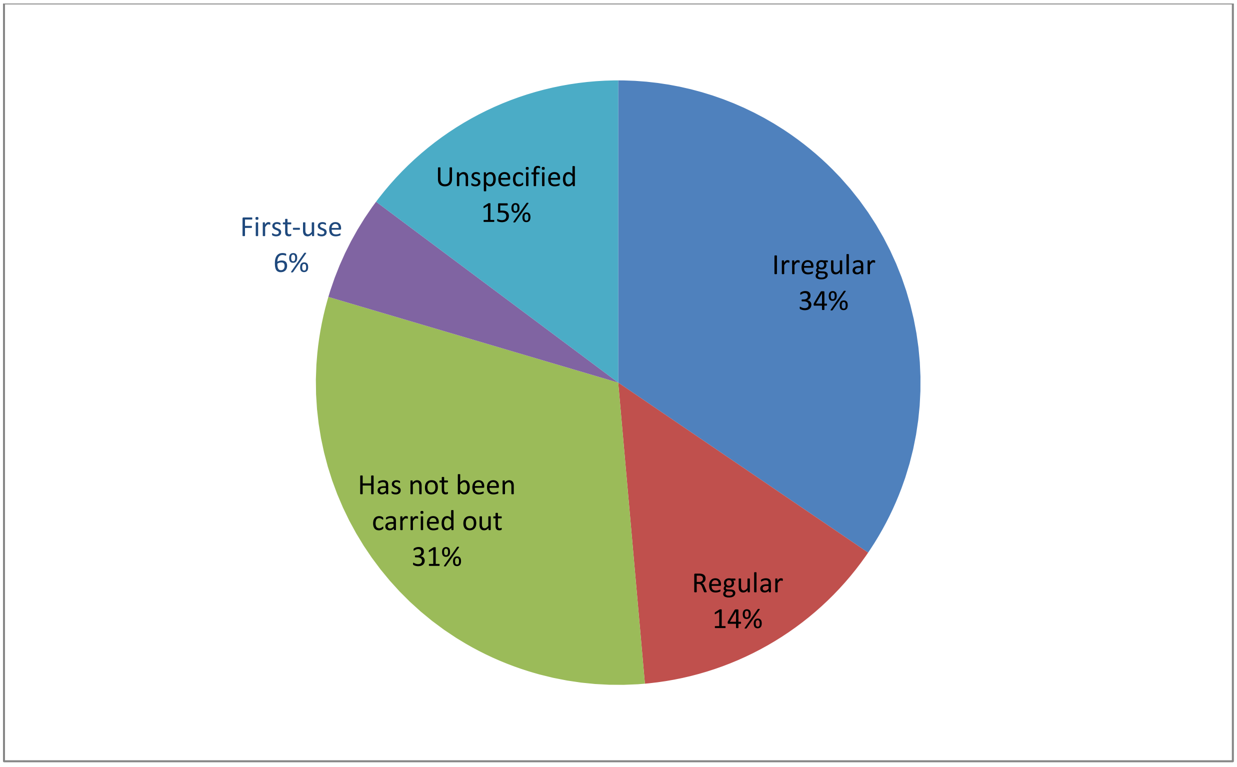


1.21 Testing frequency of availability



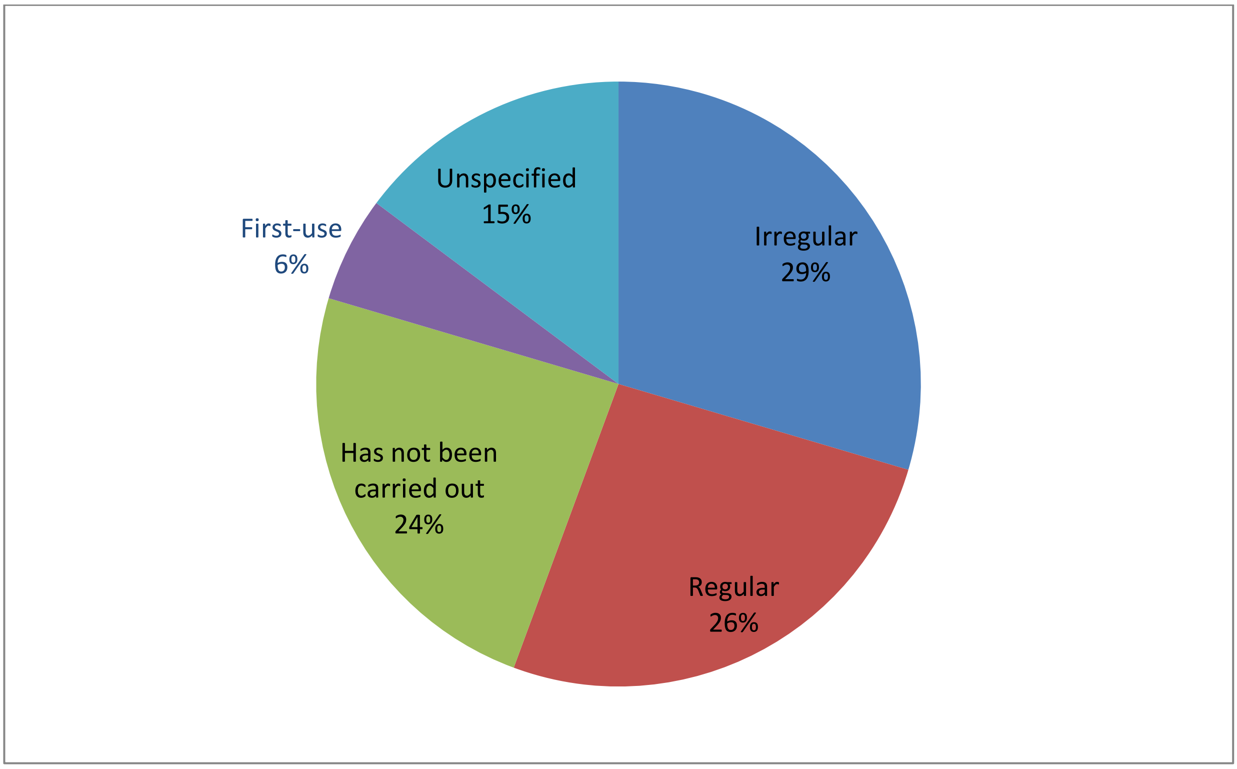
Note: availability should be tested and reported frequently, preferably independently by the customer and the provider.

1.22 Frequency of running penetration tests

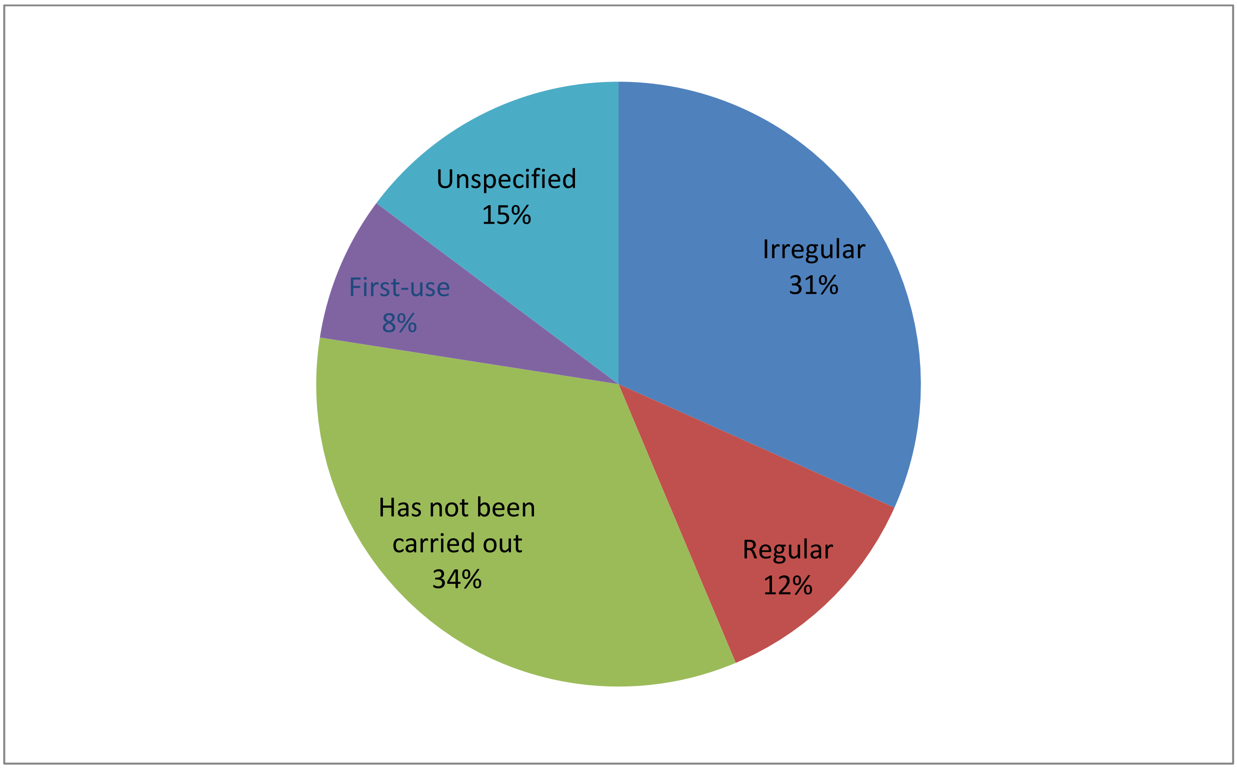


Note: customers may need permission to run penetration tests.

1.23 Frequency of running failover and backup tests

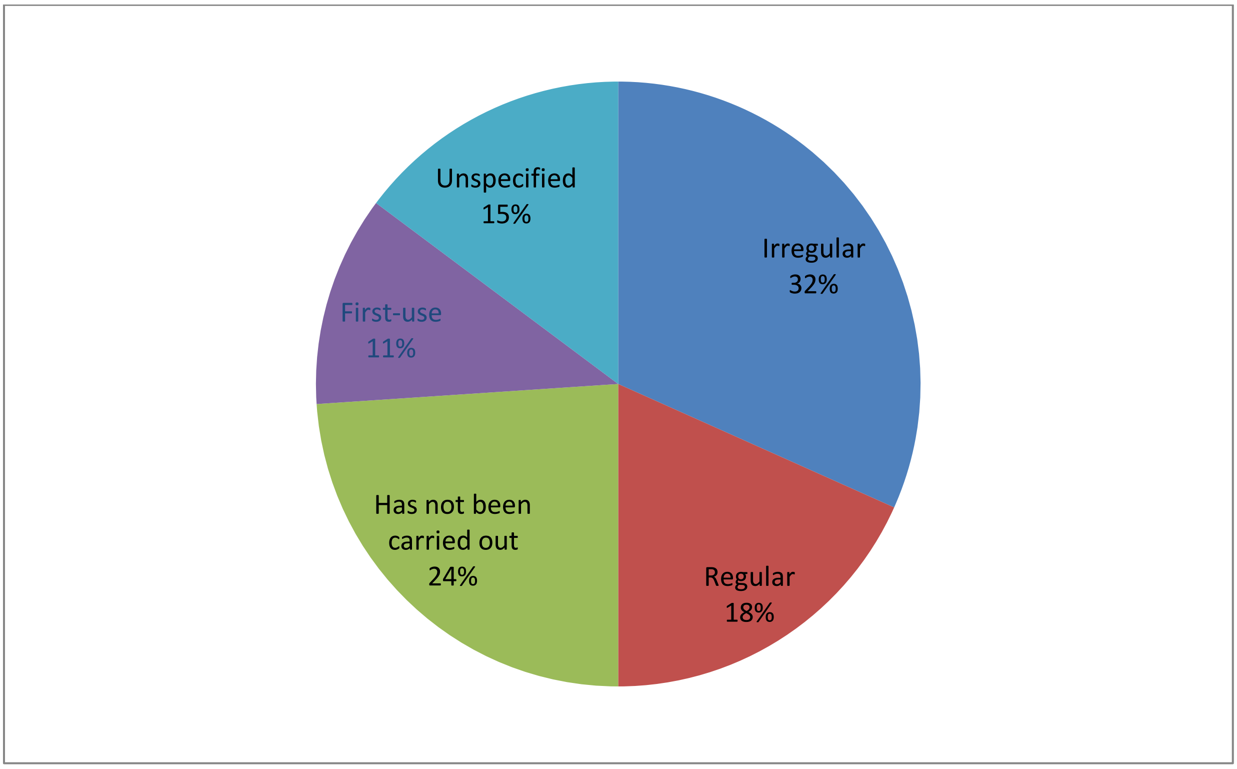


1.24 Frequency of testing data portability



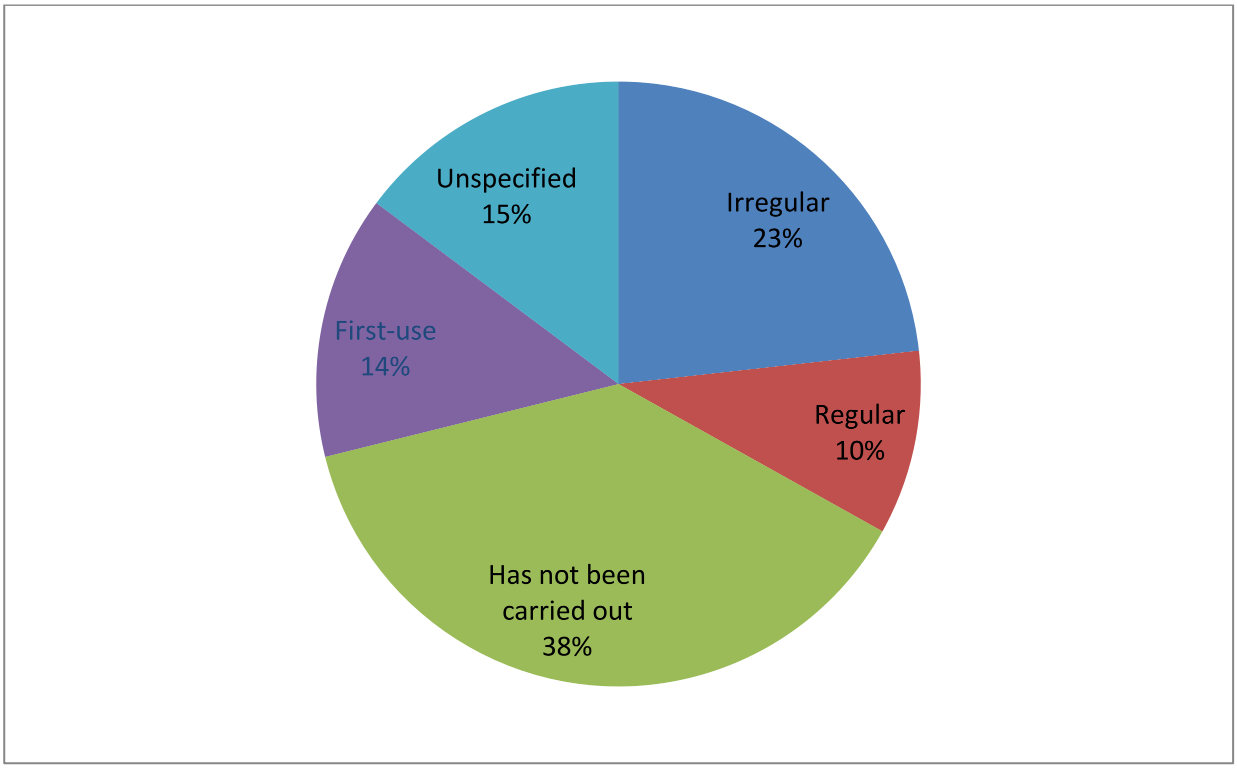
Note: aside from competition issues, data portability can be critical to business continuity in the event of a provider failure or bankruptcy.

1.25 Frequency of running load testing



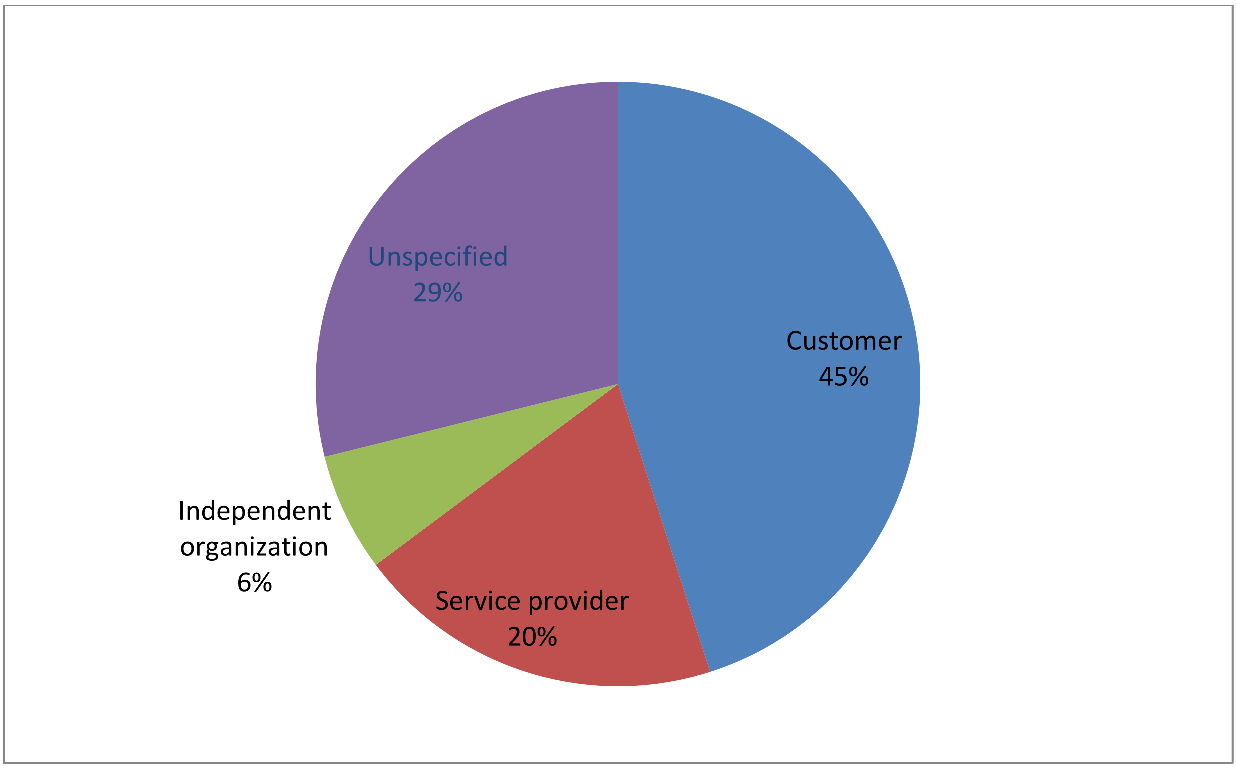
Note: for services with highly volatile demand, it is especially important to test the load tolerance of the system.

1.26 Frequency of running unit tests



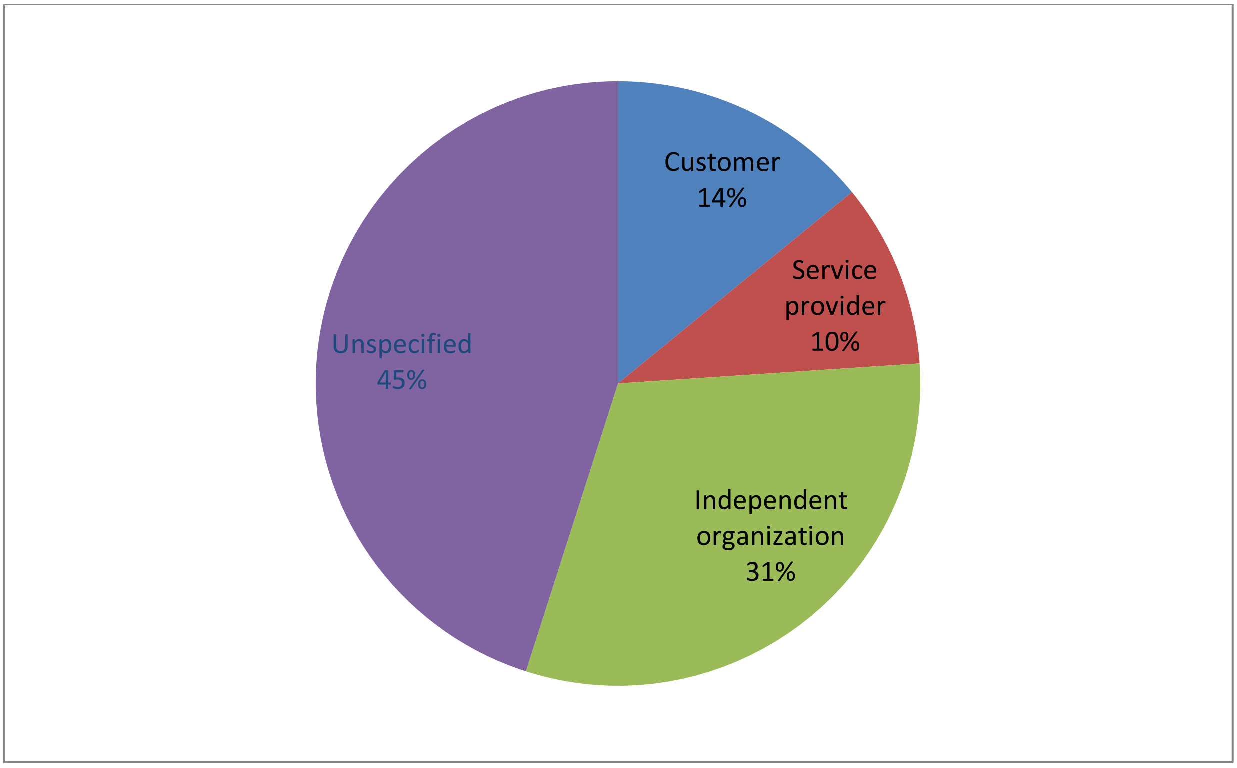
Note: unit testing ensures not only availability of network response, but the actual functioning of services according to the contract requirements. It can also test for vulnerabilities on a continuous basis.

1.27 Who carries out availability measurement?

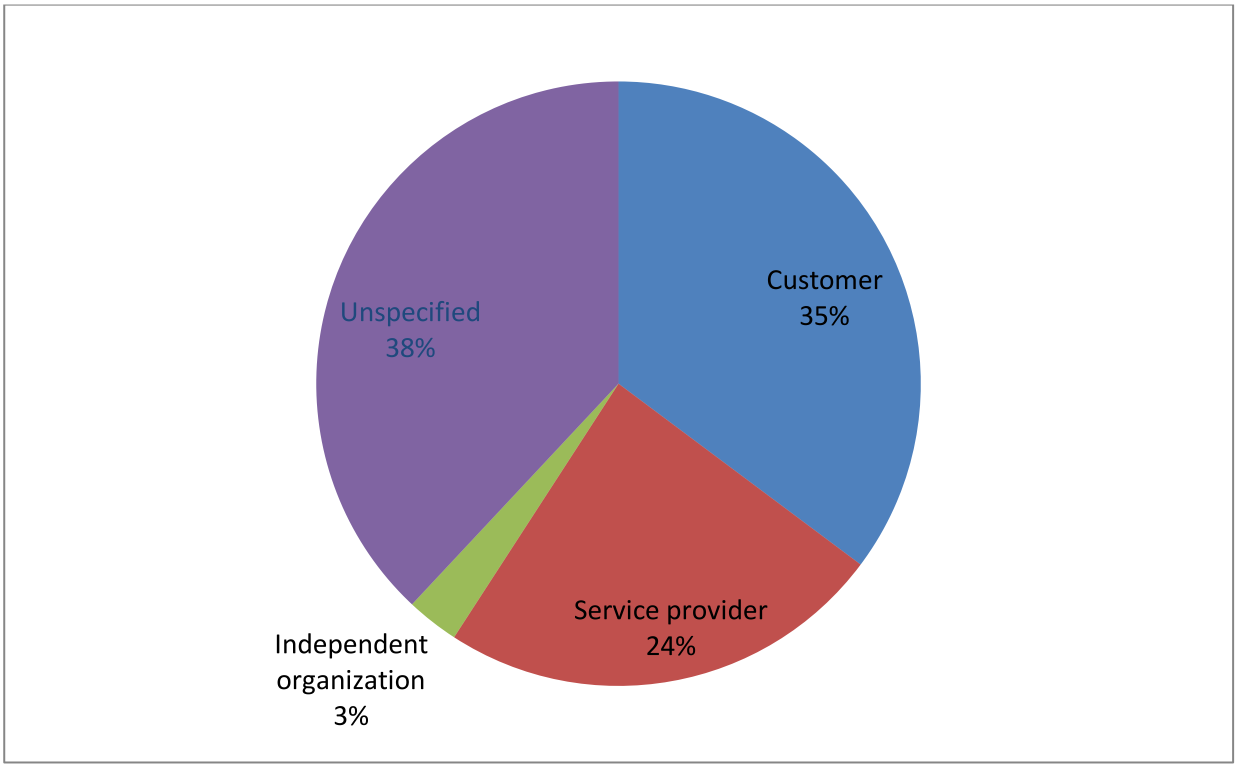


Note: In all the following, it is preferable, where technically and economically feasible that either the customer, or an independent organisation carries out the tests, either in addition to or instead of the service provider.

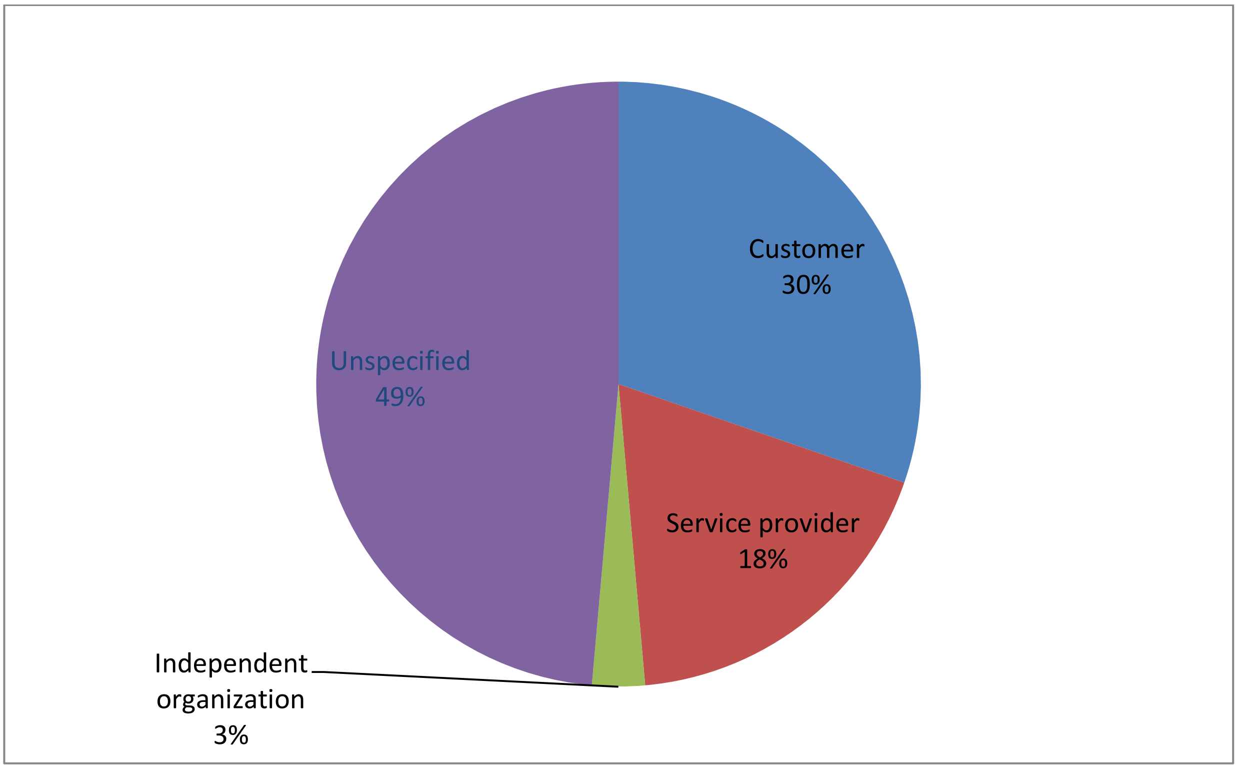
1.28 Who carries out penetration tests?



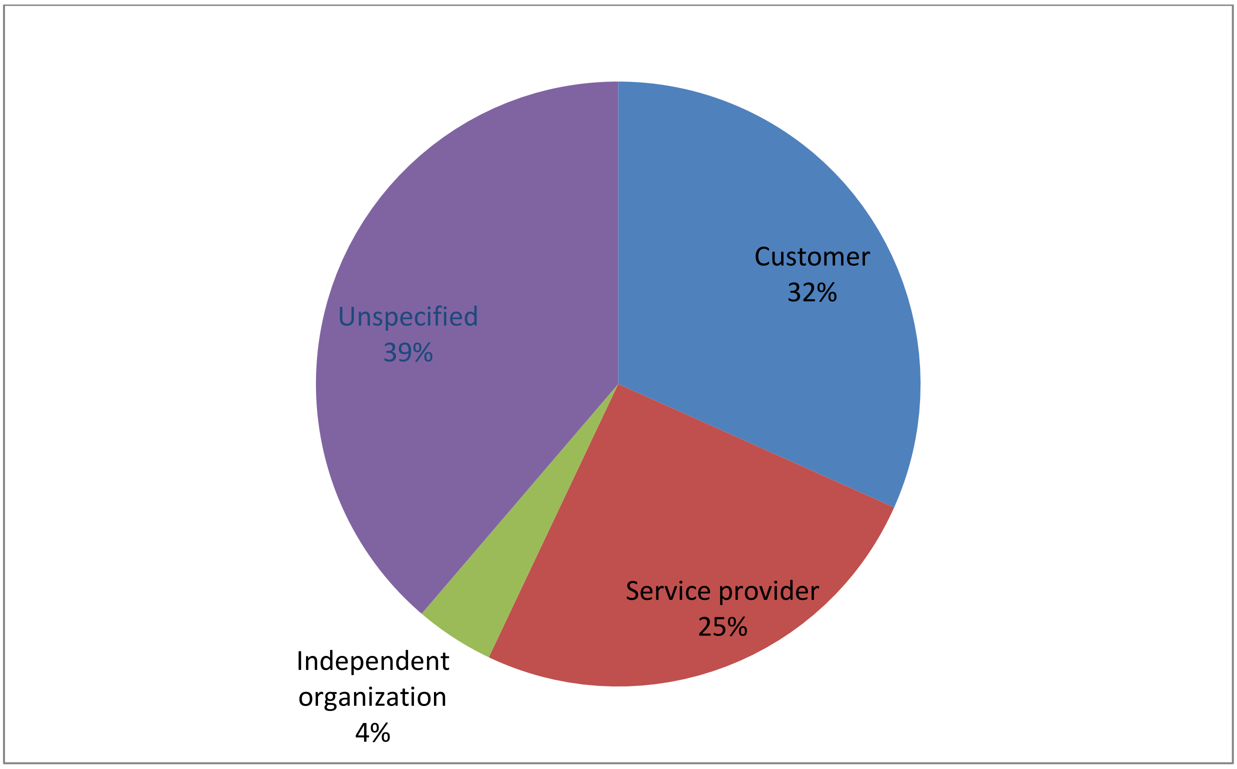
1.29 Who carries out failover and backup tests?



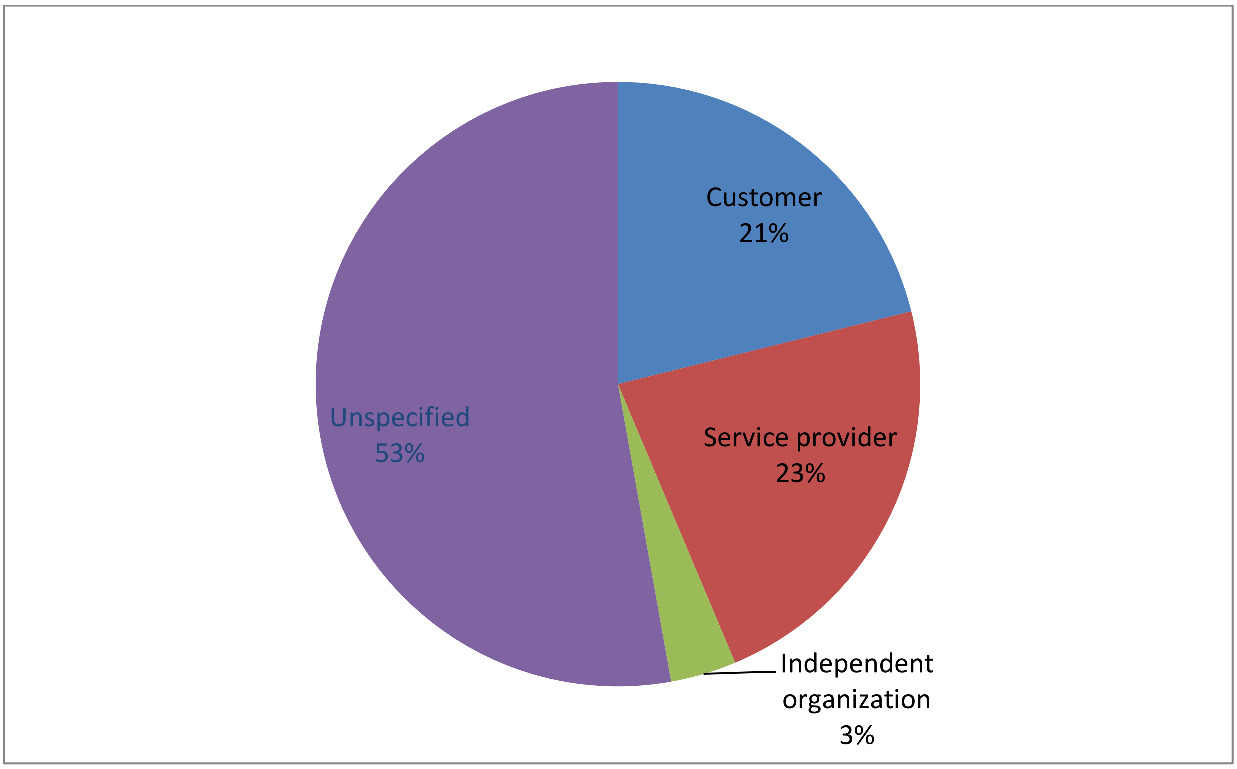
1.30 Who carries out data portability tests?



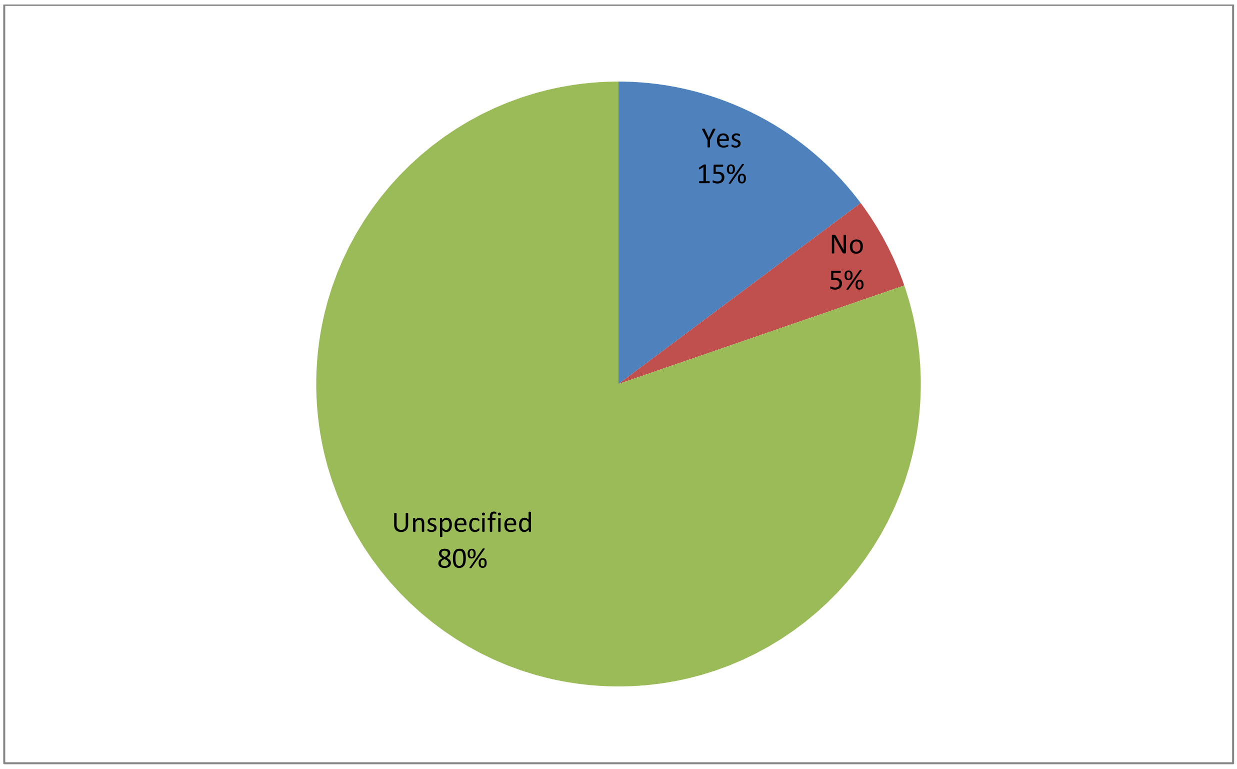
1.31 Who carries out load testing?



1.32 Who carries out unit tests?

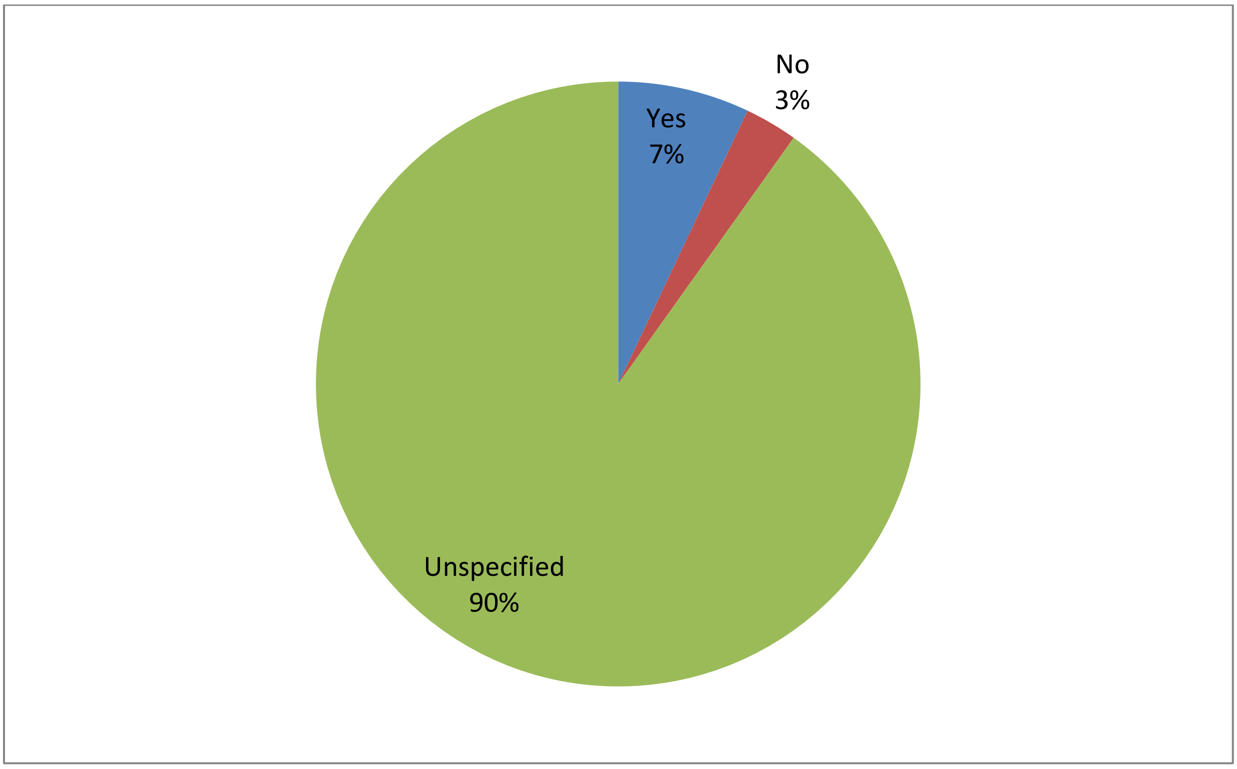


1.33 Have you received reports on availability from the provider?

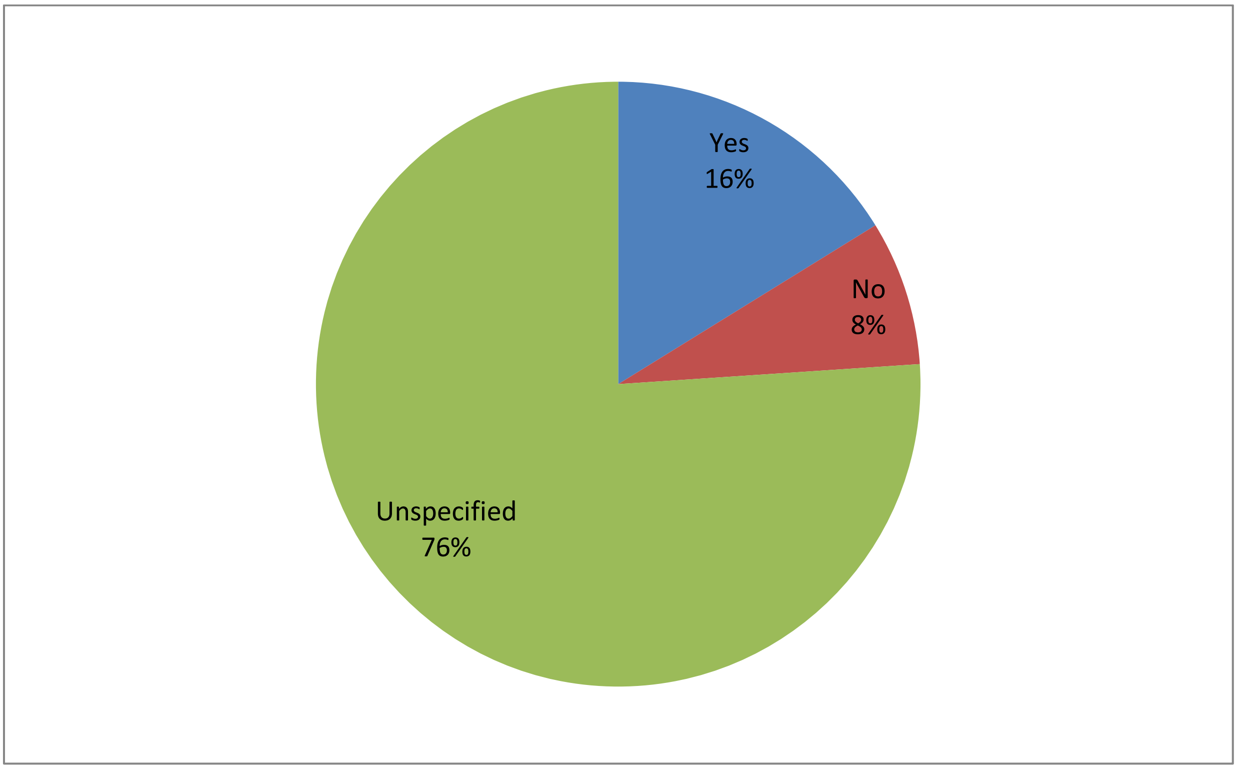


Note: Regular Service Level Reports (SLRs) and their contents should be defined. SLRs typically include for example, incidents, event logs and change reports. This applies to questions 1.33-1.36

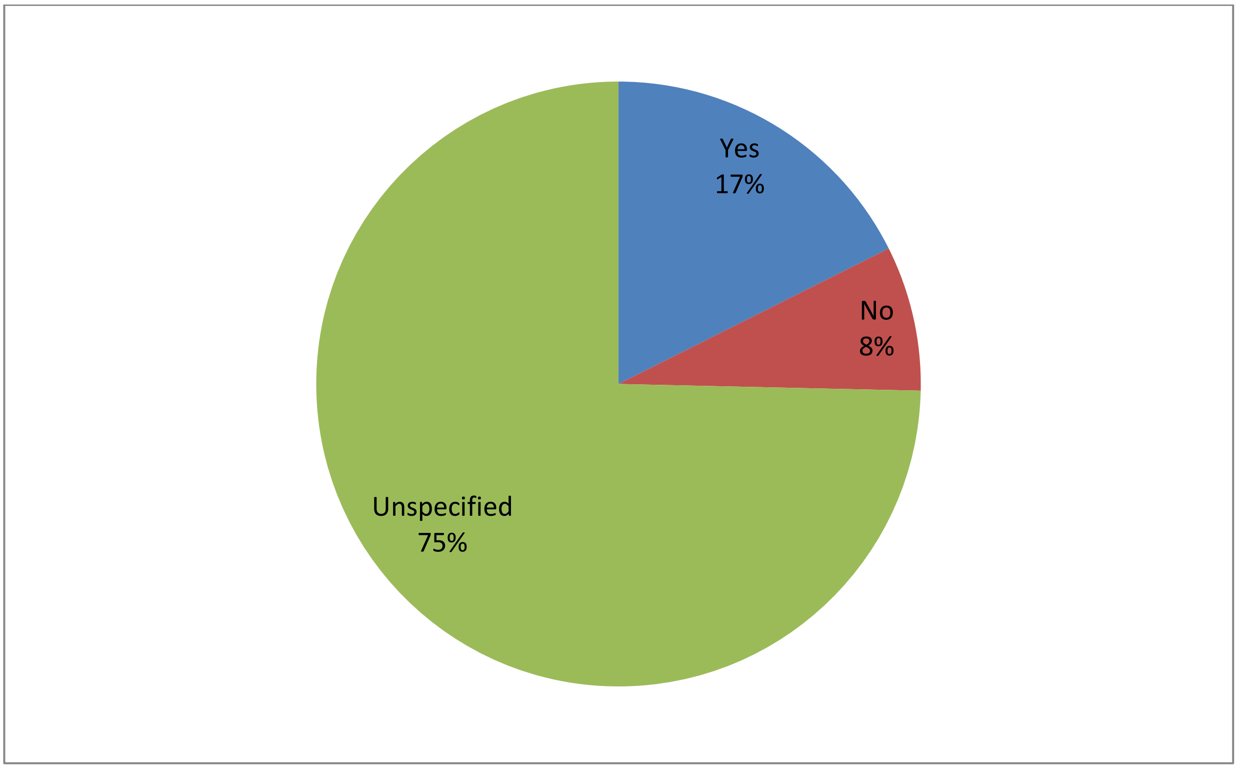
1.34 Have you received reports on penetration tests results from the provider?



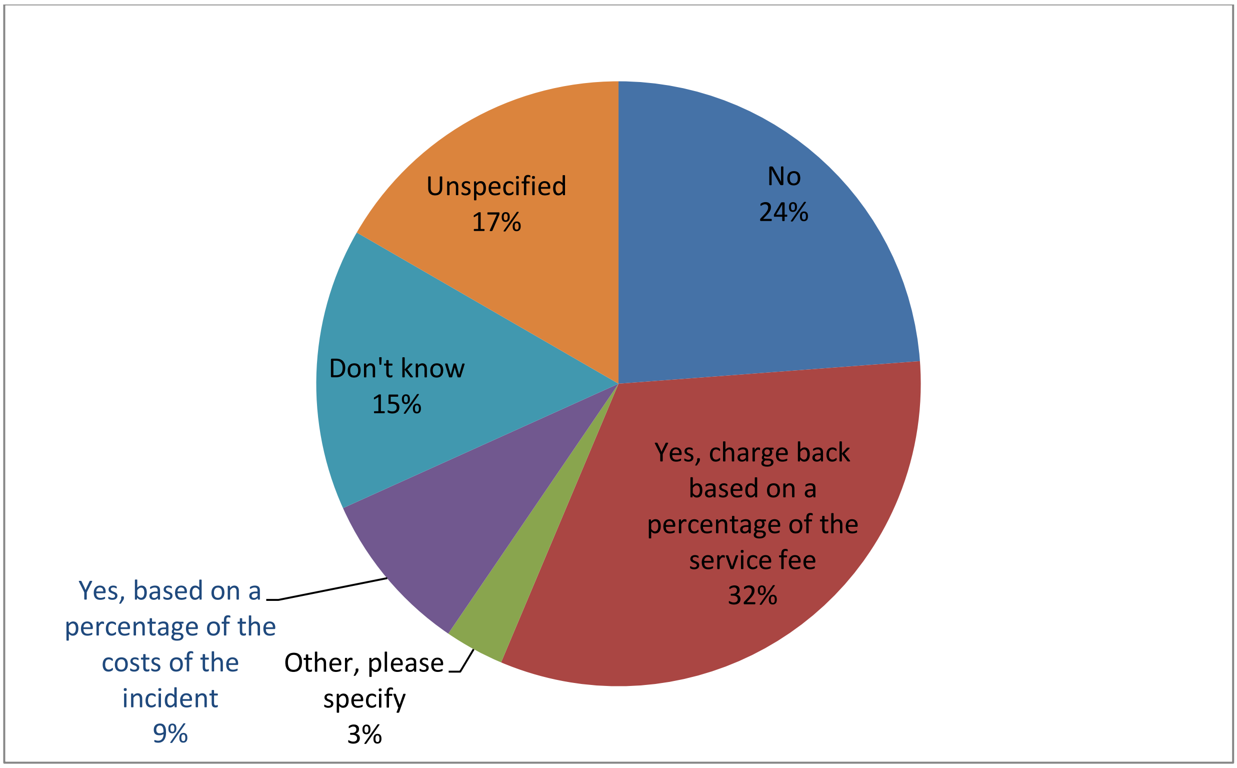
1.35 Have you received reports on failover and backup tests from the provider?



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

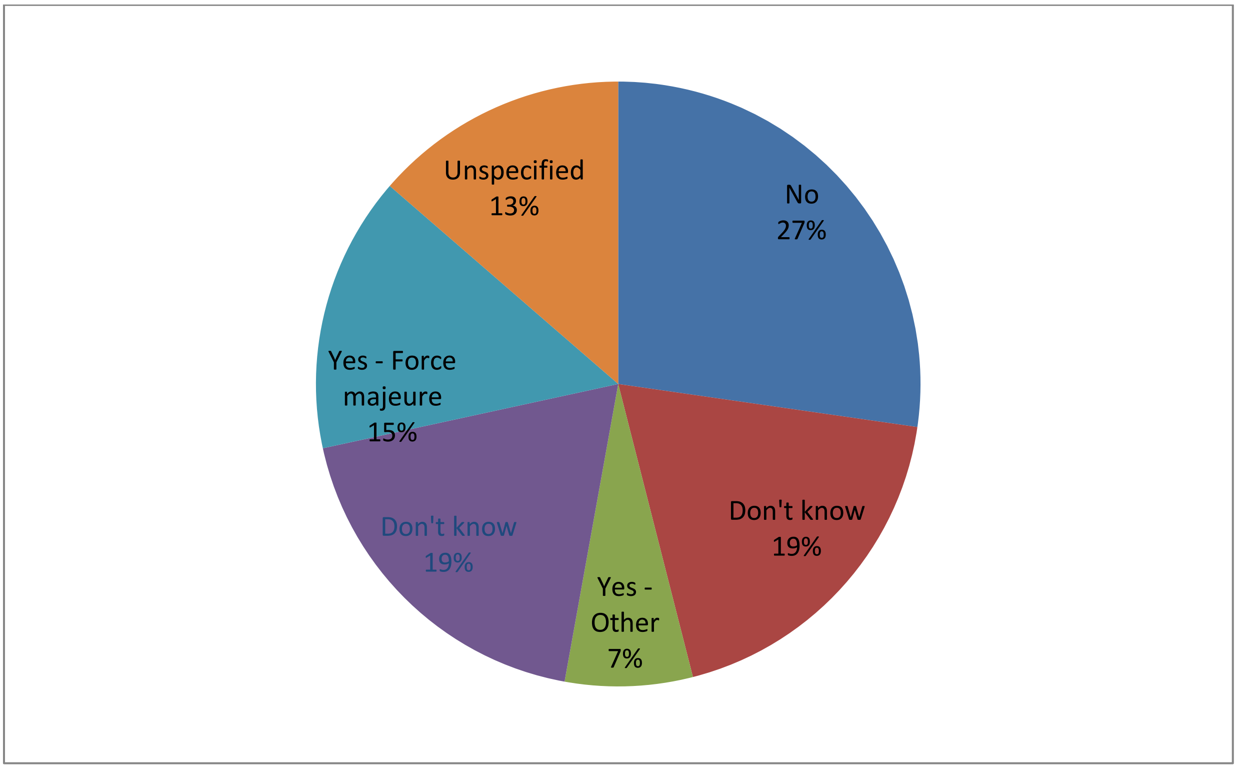


1.37 Does the SLA define penalties when the service provider does not meet the agreed service levels?

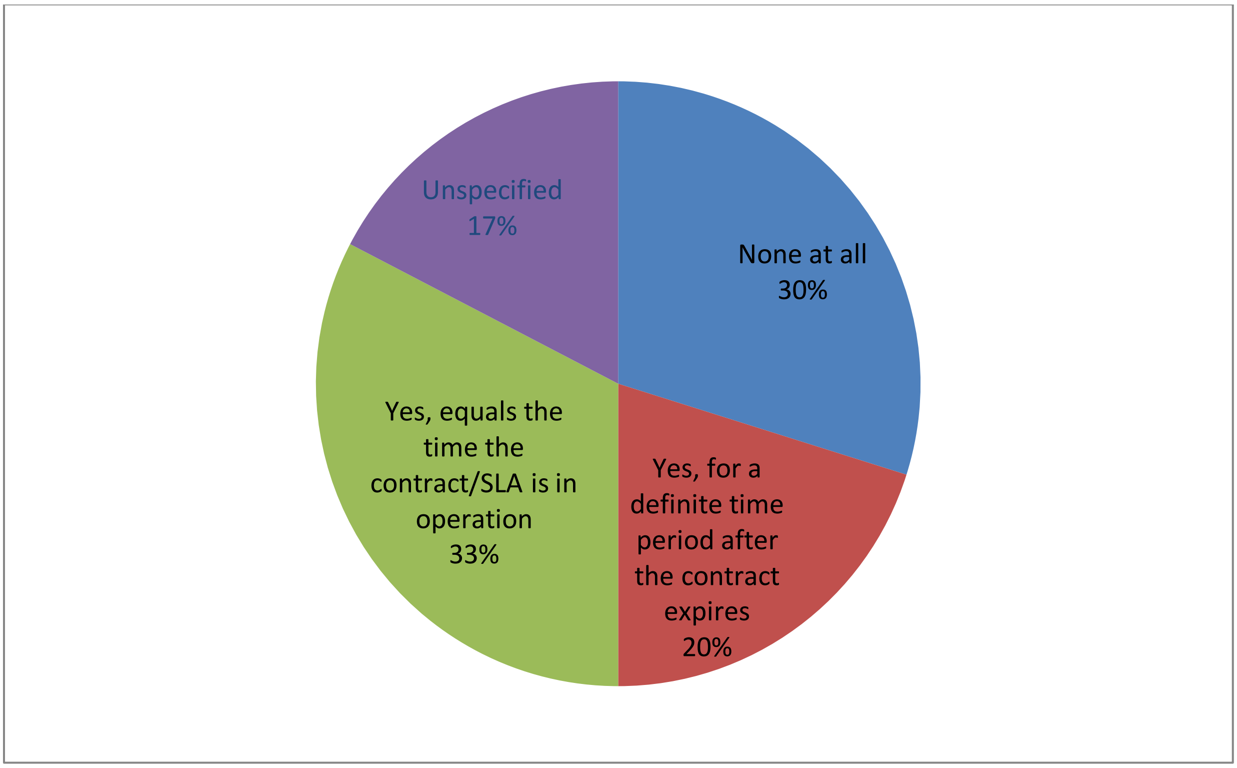


Note: depending on the setting, parameter thresholds can be linked to financial penalties, to incentivize compliance with contractual requirements or compensate for certain losses.

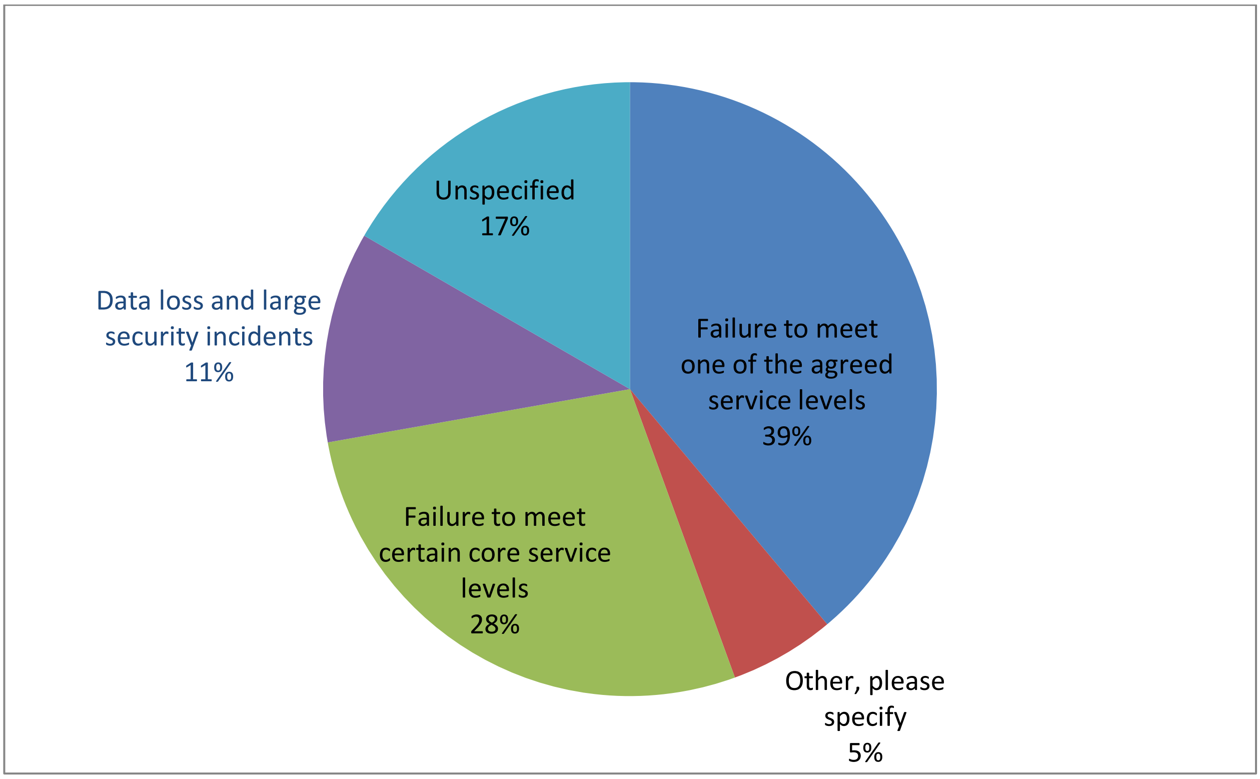
1.38 Are there penalty exclusions?



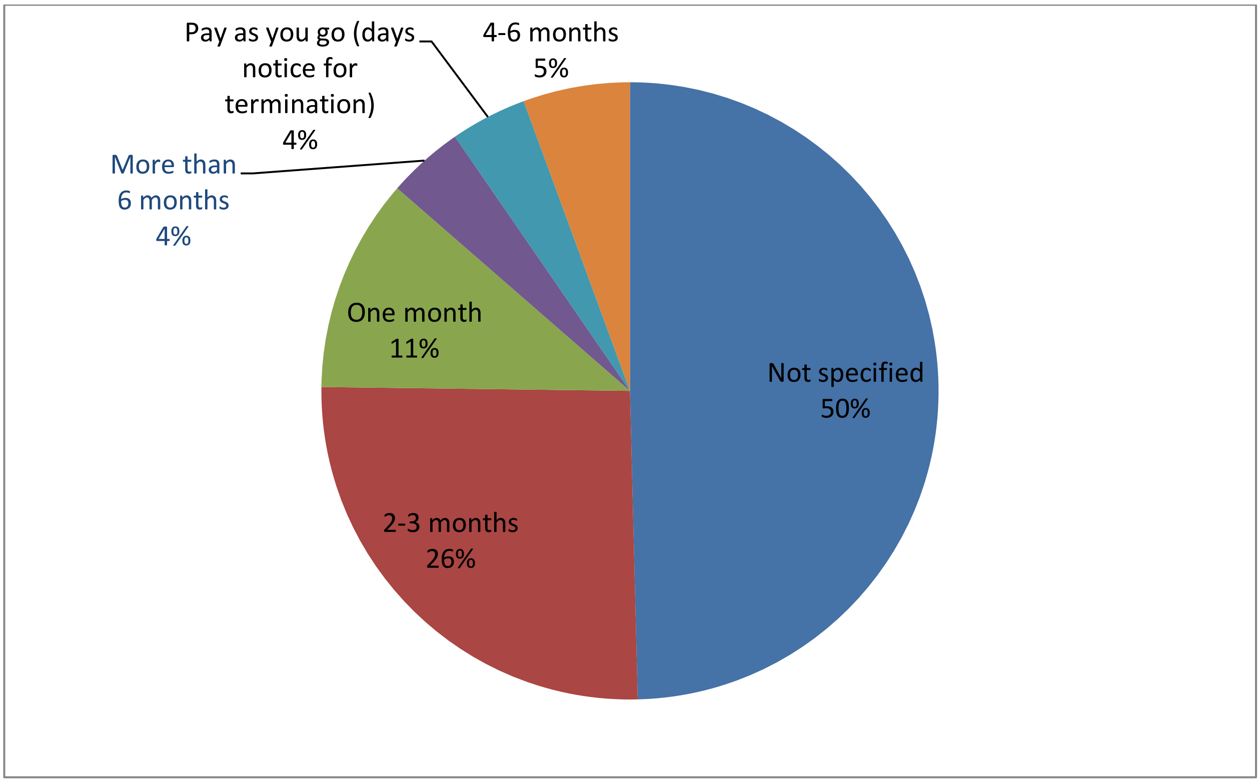
1.39 Do you have requirements in your contract/SLA on how long data must be retained and available?



1.40 When is the SLA/contract considered breached?



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



P.O. Box 1309, 71001 Heraklion, Greece
www.enisa.europa.eu