

Availability: the role of SLAs

Summary

SLAs have two roles in an organisation – defining the offer to customers and setting standards for suppliers eg in the IT supply chain.

As 3rd party IT services have an increasing role in delivery of services to customers, the relationship of the technology service provider to the organisation using it for customer or internal functions is increasingly important. A critical component of any technology vendor relationship is a service-level agreement (SLA). This defines the level of service the customer should expect, laying out the metrics by which service is measured, as well as remedies or penalties should agreed-on service levels not be achieved.

As supply chains become more complex, the provider of IaaS, PaaS or SaaS¹ will in their turn be dependent on many of their suppliers, which determine a feasible level of service delivery.

SLAs are necessary but not sufficient: SLAs are only useful after IT outages, and even then present a number of practical problems. Good practice is based on measures to anticipate, mitigate against, and recover from, outages².

SLAs in the IT supply chain

Contracts - the SLA

Most service providers have standard SLAs - sometimes several, reflecting various levels of service at different prices - that can be a good starting point for negotiation. The customer should review these, however, since they are usually slanted in favour of the supplier. For instance, a "timely" response

1

¹ IaaS hosts custom-built apps, as well as providing a general data center for data storage. PaaS is most often built on top of an IaaS platform. SaaS offers ready-to-use, out-of-the-box solutions that meet a particular business need (such as a website or email).

² <u>https://londonpublishingpartnership.co.uk/books/resilience-of-services-reducing-the-impact-of-it-failures/</u>



commitment should be quantified in the RFP³. This will affect supplier offerings and pricing and may even influence the supplier's decision to respond. For example, if you demand 99.999 percent availability for a system, and the supplier is unable to bid against accommodate this requirement, it may propose a different solution.

The SLA should cover two areas: service availability and management.

Service availability descriptions

Service elements include

- specifics of services provided (and what is excluded, if there's room for doubt), conditions of service availability,
- standards such as time window for each level of service (prime time and non-prime time may have different service levels, for example),
- responsibilities of each party,
- escalation procedures,
- cost/service trade-offs.

Management aspects

Management elements should include

- definitions of measurement standards and methods,
- reporting processes, contents and frequency,
- a dispute resolution process, an indemnification clause protecting the customer from third-party litigation resulting from service level breaches (this should already be covered in the contract, however),
- a mechanism for updating the agreement as required.

Checklist⁴: setting up SLAs

- Create separate SLAs for each IT service you need to measure and each operating unit that uses it.
- Align SLAs with the customer's desired outcome.
- Make SLAs measurable: SLAs must represent SMART goals—specific, measurable, achievable, relevant, and timely.
- Review & adjust SLAs periodically.
- Ensure SLAs account for usual & unusual exceptions.

³ Request for Proposal

⁴ <u>https://www.bmc.com/blogs/sla-best-practices/</u>



SLAs and user purchased applications

A further complication in achieving predictable availability is that in many organisations, application software can be purchased out of departmental budgets or on credit cards. The cost and resource to integrate these with existing systems is a nightmare for any IT Leader. It is common to deny support for such applications or attempt to prohibit their use. This can, however, be counterproductive, forcing users to 'go underground' when using these applications. This creates a lack of information.

How can SLAs for the IT supply chain help increase availability?

Toolkit for availability based on SLAs

In the NHS, data security is checked via the Data Security and Protection Toolkit (DSPT)⁵ that all NHS providers have to complete to provide assurance. It allows organisations to measure their performance against the National Data Guardian's 10 data security standards⁶. All organisations that have access to NHS patient data and systems must use this toolkit to provide assurance that they are practising good data security and that personal information is handled correctly.

Could a toolkit be developed for measuring and publishing availability including capturing the SLAs as specified in contracts? For use by auditors in comparing with actual availability?

Sharing SLAs vs sharing information on outages

Sharing data on SLAs would provide a common perception of expectations. It could aid during contract discussions.

In a separate paper⁷ we describe three types of information that could, if shared, improve availability. This information is "on the record" as distinct from SLA information which is aspirational.

⁵ <u>https://www.dsptoolkit.nhs.uk/</u>

⁶ <u>https://digital.nhs.uk/cyber-and-data-security/guidance-and-assurance/data-security-and-protection-toolkit-assessment-guides</u>

^{7 &}lt;u>https://www.bcs.org/media/rxdmjr5h/availability-6-report-nine-banks-data-roundtable-</u> 220425.pdf



CVSS (Common Vulnerability Scoring System)⁸ scores could be a starting point for codifying (and reporting) information about technical issues. This framework and its scoring system was developed for cyber defence purposes.

The Nine Banks data highlighted that a common vocabulary for describing the causes of outages would allow for better understanding of – particularly – common 3^{rd} party software.

The Nine Banks data also illustrated the importance of understanding the impact of IT outages. Although the period of reporting covered the Crowdstrike⁹ outage which affected many millions of people across many industries and geographies, it was not visible within the number of outages and outage duration reported. We propose that "lost user hours" could be used to share information on outages¹⁰.

Any form of data sharing across organisations requires structures and terms of reference – these are covered in a separate paper¹¹.

Defining the offer to customers via SLA

Not all systems need to provide 99.99% availability. And no service can achieve 100% - like cars, IT systems need to be "off the road" occasionally for preventive maintenance.

Visibility of availability standards set as appropriate to the service, and levels actually achieved, could use the metrics of SLAs.

The NIS2¹² Framework applies to all CNI organisations, but regulation has not yet specified threshold "lost user hours" for reporting purposes. Would an SLA visible to the public for all suppliers in the sector provide assurances to customers? This might be expressed – as for train services – in terms of outage duration leading to recompense to individuals.

Could there be a role for industry sector regulators to agree on availability standards for services, defined through an SLA, within each sector?

4

⁸ <u>https://nvd.nist.gov/vuln-metrics/cvss</u>

⁹ https://www.bbc.co.uk/news/articles/cr54m92ermgo

¹⁰ <u>https://www.bcs.org/media/czwjt34u/availability-the-nis-framework.pdf</u>

¹¹ <u>https://www.bcs.org/membership-and-registrations/member-communities/bcs-it-leaders-forum/papers/</u>

¹² <u>https://www.nis-2-directive.com/</u>