

DoD ESI White Paper

Service Level Agreement (SLA)  
Best Practices and  
Contractual Considerations

---



## About DoD ESI

The DoD ESI was formed in 1998 by Chief Information Officers at the DoD. To save time and money on commercial software, a joint team of experts was formed to consolidate requirements and negotiate with commercial software companies, resulting in a unified contracting and vendor management strategy across the entire department. Today, DoD ESI's mission extends across the entire commercial IT life-cycle to include IT hardware products and services. DoD ESI has established DoD-wide agreements for thousands of products and services.

[www.esi.mil](http://www.esi.mil)



## Executive Summary

### What happens after signing a contract?

The execution of a contract marks the starting point of services to be provided from either a new service provider or from an existing service provider. Whether these services are being provided during the formation of a new supplier relationship or within the framework of an existing supplier relationship, you are relying upon the supplier for your service needs. This reliance creates a risk exposure that can be mitigated by having a robust Service Level Agreement (SLA) in place.

Even though you may have an underlying contract that governs the services, that contract may not be detailed enough concerning the tactical items you expect to encounter once operations and services begin. Therefore, it is best to negotiate and fully understand key expectations for all service components upfront. Such items include:

- What are the specific services to be provided?
- Where will the services be provided?
- Who will provide the services?

- What are the acceptable standards for each service being provided?
- How are these standards measured and reported on?
- What happens if the services are not provided according to the acceptable standards?

If expectations for the various service needs you contracted for are not well defined and monitored, including the standards of performance and the metrics for them, your position for enforcing the contract will not be as strong as when you have a robust SLA in place before services begin. SLAs ensure a good poll position or starting gate for your services.

Knowing how to include service levels into your contracts, either as part of the underlying services contract or as a standalone agreement, will help mitigate the inherent risks of using a service provider and enable easier enforcement of your contract provisions.

---

## Table of Contents

<b>What is a Service Level Agreement?</b> .....	<b>4</b>
<b>Use Cases</b> .....	<b>4</b>
<b>Contents of a Standard SLA</b> .....	<b>4</b>
<b>Two Primary Types of SLAs for Software Systems</b> .....	<b>6</b>
<b>Support Service Levels</b> .....	<b>6</b>
<b>System Availability and Performance Service Levels</b> .....	<b>10</b>
<b>Cloud Specific Terms</b> .....	<b>12</b>
<b>Additional Considerations</b> .....	<b>13</b>
<b>Conclusion</b> .....	<b>14</b>

## What is a Service Level Agreement?

A Service Level Agreement (SLA) is a contract that defines clear service expectations in measurable terms and sets obligations for when expectations are not met (e.g. hold harmless termination rights, liquidated damages, credits, etc.). Normally, an SLA attaches to an underlying agreement, such as a Master Services Agreement or Software License Agreement, in the form of an Annex or Attachment. Sometimes, SLAs might attach to a particular Statement of Work (SOW). The SLA serves to augment the underlying agreement with specific performance standards in various ways as described in this white paper.

## Use Cases

Since SLAs provide a mechanism for assuring acceptable levels of performance, they should be used anytime quantifiable, measureable, performance based services are being provided. Without an SLA in writing, it may be harder to enforce obligations if the service is not performed or delivered as expected. Some examples of performance based services where an SLA should be used include: (i) Managed Services Agreements; (ii) Software Maintenance and Support Agreements; and (iii) Hosting Agreements.

Although SLAs are typically used to help manage external service providers, they can also be used internally within an entity to provide assurances to other departments or lines of business that services will be provided at agreed upon levels of performance. For example, a Business Intelligence and Analytics Department may have a one month SLA for new custom report requests by other departments.

## Contents of a Standard SLA

These are the typical contents of a standard SLA document:

**Preamble** - This SLA component is an introductory narrative describing the overall purpose and objective(s) of the SLA.

**Service Item Measures and Descriptions** - This section of an SLA is where each service item is clearly listed by name and fully described as to what service item is being measured. If the underlying contract or SOW already clearly defines each service item, you can reference back to that contract in the SLA by providing the unique name of that service item in the listing.

Having a well-defined and clearly written services description for each service item of the contract is a critically important prerequisite to having an effective SLA. This section should also identify any new definitions needed in order to provide a clear understanding between the parties for what is to be delivered for each service item measure.

For example, what constitutes a “day” or “standard hours”? Are these business days, calendar days, are holidays included? Which holidays apply (e.g. your service provider may follow a different holiday schedule, especially if they are operating in a different country). Do you and the service provider have the same understanding, a true meeting of the minds?

**Service Levels** - This component of an SLA identifies the performance objectives and acceptable standards, levels or thresholds for each service item. These are typically described via metrics per service item being measured. For example, "The quality of software code that the service provider develops and delivers as an end product must be 99% void of any bugs or other harmful agents such as security vulnerabilities."

**Measurement and Reporting** - This section of the SLA shows how the acceptable standards and metrics are measured and monitored.

For starters, some examples of service item measures as extracted from the GSA's SLA Reporting Tool - GSA Q1 FY 2014 include the following Helpdesk category of services (these have been slightly modified to add language for acceptable standards):

- **First Contact Resolution** - Percentage of contacts (telephone calls) to the Helpdesk that are resolved by a live agent on the first contact; "resolved" means the caller agrees, at the end of the call, that the issue/inquiry has been answered by the Helpdesk. Acceptable standard = [x]% of calls per rolling 30 day period.
- **Abandonment Rate** - Percentage of telephone calls to the Helpdesk abandoned by the caller after the caller selects the option to speak to a live agent. Acceptable standard = [x]% of calls per rolling 30 day period.

- **Number of Tickets Escalated** - The number of tickets that are opened with the Tier 2 or 3 Helpdesks. Acceptable standard = [x] tickets per rolling 30 days.
- **Ticket Resolution Time** - Period of time from when the ticket is first opened with the Tier 2 Helpdesk until the ticket is resolved or closed out by the Tier 2 or Tier 3 Helpdesk. Acceptable standard = [x] minutes.

Wherever possible, keep the metric calculations used to measure service level adherence as simple as possible. However, sometimes that advice (keep it simple) is nearly impossible to follow. Since some service level calculations can be complicated, it is best to provide an example of the calculation within the SLA. Providing calculation examples in the SLA helps to ensure that the parties interpreting and enforcing the service levels are doing so consistently and correctly.

This section should also describe the methodology used for monitoring, analyzing and reporting how the actual service being delivered is measuring up against the acceptable standards. It is important to clearly identify the party responsible for measuring, analyzing and reporting the performance data for each service item. Other questions addressed in this section include, what is the frequency and method for reporting, how will the reports be communicated, and who is the proper audience to receive these reports. This includes specifying the frequency of updates expected while an issue is being resolved.

If the service provider is the one responsible for reporting on whether or not they met the service levels, be sure that your organization has an independent tracking mechanism to validate the service provider's reports against. Finally, be sure to specify the start and end timeframes for each measurement (e.g. Ticket Resolution Time is measured from the time a call is placed to the help desk, an email sent to the help desk, or a ticket created in the issue system until the end consumer has confirmed that the ticket is indeed resolved).

### **Obligations for SLA Failure**

Now that you have started drafting an SLA for a project that you are working on, and you have the introductory preamble, the service item descriptions, service levels and measure and reporting methods all articulated, what else is needed as part of the SLA? The missing section that gives all of the groundwork established by the preceding sections of the SLA more emphasis and power can be referred to as the "teeth" or the service provider's "skin in the game."

This final section of an SLA is the most important, because it creates motivation for the service provider to ensure your specified service levels are met. This section provides that assurance by spelling out specific obligations and remedies for failing to meet service levels. These remedies may come in many different forms, such as: free fixes, service credits, or refunds (if allowed). If seeking liquidated damages as a remedy, ensure the acceptance of liquidated damages does not limit your ability to seek other remedies, including contract termination and release.

This section may also include templates that should be used when submitting a claim or an acknowledgement that the service provider failed a service level and the remedy that is being requested for such failure (e.g. requesting credits be applied to your next monthly invoice). Such service credits are normally limited to the total annual amount paid or to a percentage of the service item fee.

## **Two Primary Types of SLAs for Software Systems**

So far we have examined the general SLA standards for three SLA use cases: (i) Managed Services Agreements; (ii) Software Maintenance and Support Agreements; and (iii) Hosting Agreements. Now we will fine tune our focus to look at the two primary Software System SLA types that might be used in any of the three use cases – and the specific SLA standards for both types:

- 1. Support Service Levels** - Used primarily for managing software issue reporting (end user functionality or technical support issues), service provider responses, updates and final resolutions.
- 2. System Availability Service Levels** - Used to define a system's availability or "uptime" and expected levels of performance (e.g. throughput quantity, processing times and overall capacity).

### **Support Service Levels**

Software support typically includes post-sales services provided by a software publisher or vendor in solving software conflicts, breaks, bugs, and usability problems, and in supplying remote troubleshooting via phone, web or automated tools.

**Understand the Support Model** - One of the first steps in creating service level terms for support agreements is to fully understand the service provider's support model and the various service items that are included. Software support providers usually offer various levels of support that differ by the number, type or delivery time of services included in the cost for support (usually, an annual cost for software purchased in perpetuity). For example, a service provider's support options may look similar to those listed in Diagram 1 below:

**Diagram 1:** Service Provider Support Options example.\*

\* Severity levels and resolution times may be included in a matrix such as this or would need to be defined elsewhere in the SLA. They are purposefully left out of this diagram to focus on the various support models, since response and resolution times typically vary depending on level of severity.

Service Item Name (as defined elsewhere in SLA)	Standard Support	Gold Support	Platinum Support
<b>Versions supported</b>	Current major version plus prior major version maintenance release	Current major version plus prior major version maintenance release	Current major version plus prior major version maintenance release
<b>Error correction</b>	Yes	Yes	Yes
<b>Non-error support (typically for customizations)</b>	6 support cases/year/customer	10 support cases/year/customer	Unlimited support cases
<b>Hot fixes and minor releases</b>	Yes	Yes	Yes
<b>New Major releases</b>	Yes	Yes	Yes
<b>Priority for enhancement requests</b>	Medium	High	Highest
<b>Response time for support issues</b>	2 hours, if within standard service hours	1 hour, if within standard service hours	30 minutes, if within standard service hours
<b>Emergency reporting</b>	No	Yes, within Gold extended service hours.	Yes, within Platinum extended service hours.
<b>Response time for emergency support requests</b>	N/A	2 hours if emergency request during Gold extended service hours	1 hour if emergency request during Platinum extended service hours
<b>Standard service hours</b>	7:30 AM - 5:30 PM M-F Eastern Time	7:30 AM - 5:30 PM M-F Eastern Time	7:30 AM - 5:30 PM M-F Eastern Time
<b>Extended service hours</b>	N/A	7:30 AM - 5:30 PM Sat and Sun Eastern Time	All hours other than normal service hours

**Confirm the Actual Support Provider** - After understanding the service items that will be provided under the chosen support option, the next step is to confirm who is providing your support. Do not assume that the support provider is the direct software producer (the Software Publisher) or the reseller you purchased your support from. Ask who will be answering the other end of the support hotline, email or ticketing system and where they are located. Also ask if your support option entitles you to a dedicated support resource or team that is responsible for knowing your software instance, responding to your issues and following up on final resolution. Also identify where their support centers are located. This is useful to know, especially if their support centers are offshore. In some cases, the DoD and Federal agencies will preclude the service provider's use of offshore support centers and may impose additional security requirements.

**Resolution Timing** - A key component or service item that is normally added to Diagram 1 above is the resolution time for support requests. Ultimately, the end user not only wants to know that their issue is being worked on (responded to), but they really want to know when their issue will be resolved. Think of these two items, response and resolution, as going hand-in-hand. One way to remember them is "R&R." In the technical support world, for the most critical support issues, there is no rest and relaxation until your support request is responded to and resolved.

**Severity Levels** - Before being able to list the response and resolution times per level of issue severity, the support service items must be segmented into criticality. One approach is to separate these criticalities into three levels.

An example of severity levels is listed here:

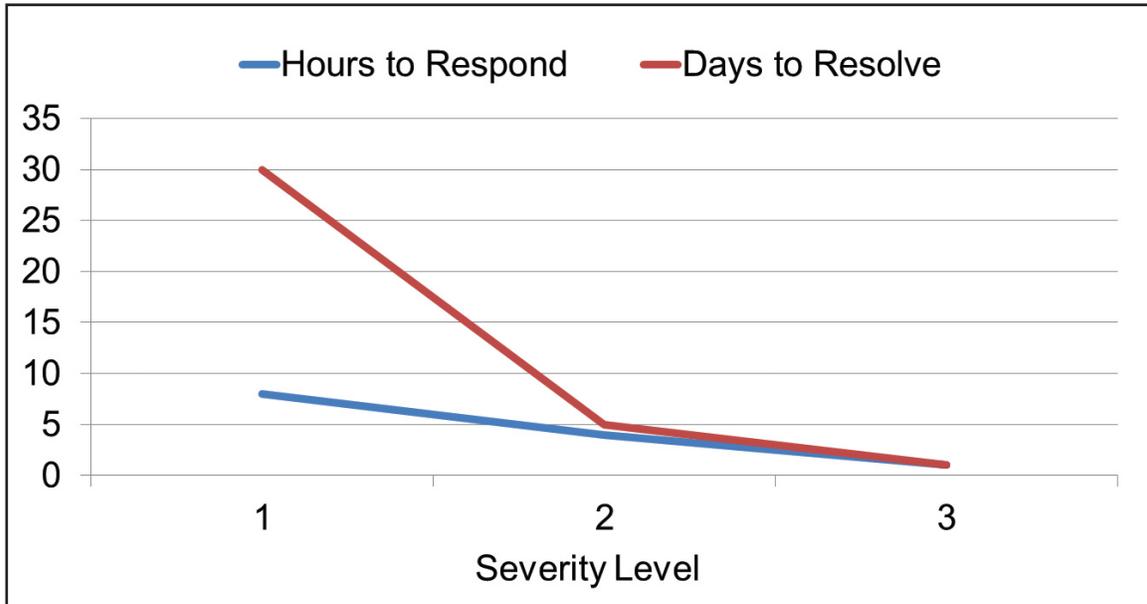
- Level 1 – Any issue impacting one or more users.
- Level 2 – Critical issue impacting a key process where a workaround is available.
- Level 3 – Critical issue impacting a key process where a workaround is not available.

Some additional guidance when segmenting and defining severity levels includes:

- Making severity level setting explanations as objective as possible.
- Providing support incident examples in the SLA, but be careful not to list too many examples, since by listing too many, if an incident occurs that is not on the list, the support provider may claim it is not covered (a rare occurrence, but one to avoid where possible). Instead, list one or two examples, but recognize that these examples may need to be updated as support options and needs change over time.

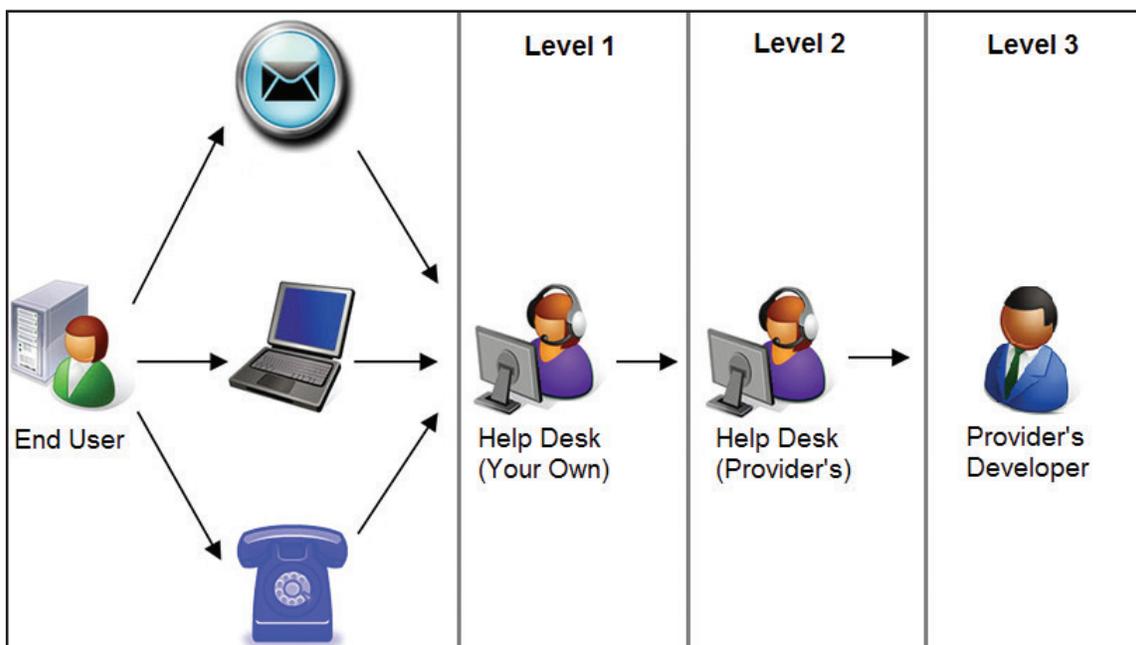
Once severity levels are identified and agreed upon, establish metrics for acceptable response and resolution time for each severity level. For example, "All reported Level 3 severity issues will be responded to within 1 hour and resolved within 4 hours." If a support incident cannot be readily bucketed into a particular severity level, ensure that the level setting is mutually agreed to. Also, for all support incidents ensure that the resolution timeframe is not contingent on the support provider having remote access into your environment.

**Diagram 2:** Example of Response and Resolution times per Severity Level.



**Support Incident Flow** - Another section that a support service level agreement should include is the identification of the support request flow. Some support providers' help desks require that only trained users or your organization's help desk personnel are allowed to submit a ticket for support.

**Diagram 3:** Example of Levels of Support and Flow of Support Requests/Tickets.



**Notifications to Support Provider** - This section of the support service level agreement should list key contacts and the escalation process that can be used in the event of a support request failing to meet the requisite service levels agreed upon for response and resolution timing.

- **Key Contacts** - List all account management and technical support contact information, including mobile phone numbers. This information will change over time, but it is a good practice to include it in the SLA. The information should be reviewed several times during the year to ensure it is up to date.
- **Escalation Process** - Ask the provider to define their escalation process and draft it into the SLA, so other persons within your organization will have a clear escalation path and know who to contact. This helps to provide information to others who will need to carry on supplier management responsibilities after the initial project team has installed the software.

### **ESCALATION CONTACTS**

- 1 – Account Representative
- 2 – Senior Account Representative
- 3 – Regional Support Manager
- 4 – VP of Support
- 5 – COO or CEO

- **Ongoing Management** - Have the provider contractually commit to at least a monthly call or meeting to review service performance, SLA metrics and any service issues. Also, keep an independent “issues” log to match up against the provider’s ticketing system in case there are discrepancies. (Their reporting versus yours).

**Notifications from Support Provider** - While specifying the flow of support incidents, list the expectation that “immediate notification” is required for new issues or vulnerabilities that the support provider is aware or should be aware of (e.g. a bug the support provider learned about via another client). Part of this notification process is identifying how the support provider is to contact you. One approach for solving this is to set up an email distribution list within your organization’s directory that the support provider can use for all notifications (e.g.[software] notifications@department.gov).

### **System Availability and Performance Service Levels**

In addition to all of the service level components listed above in the “Support Service Levels” section of this paper, the following components should be added for system availability and performance service levels. These are applicable where a service provider is hosting your software or providing other services that are not controlled in-house (e.g. network connectivity).

**System Uptime and Performance** - As the title indicates, there can be two aspects of what is often referred to as system performance. One is called system availability or system up time (connectivity) and the other is usually referred to simply as system performance or system response time (capacity and throughput responsiveness). It is more common to see SLAs for system up time than for system performance, but it is possible to include both in your SLA.

To avoid confusion, it is imperative that the terms “system uptime”, “system availability”, “system performance” and “system response time” are clearly defined.

In simple terms, the availability of a system is the percentage of time that a system is expected to be traversing data via connectivity. This percentage of uptime or system availability would be the key metric for this SLA. A calculation example for system availability could be  $= 1 - (\text{total connection outage time}) / (\text{total expected in-service connection time})$ .

System performance or response time is often expressed as the amount of time it takes for a keystroke to be acted upon by the system or the amount of time it takes for a transaction to be processed. In other words, is the system responding quickly enough to the requests it is receiving and does it have the capacity to handle peak load demand? We have all experienced the appearance of an hour glass or similar “system is processing” symbol on our screen indicating the system is processing the last instruction we entered. The key metric for this SLA is usually expressed as a unit of time. A few calculation examples for system performance could be  $= \text{actual batch processing time vs. expected batch processing time}$ , or  $= \text{actual report processing time for query [x] vs. expected report processing time for query [x]}$ .

It is important to reiterate that uptime of a system is not the same as a system’s performance levels. For example, you might have an email service provider in the cloud that is up and running (meeting “uptime”), but your email messages are being delayed by four hours (slow system performance and/or network issues). If system performance, as we have defined it, is part of your overall System Performance and Uptime SLA (and we recommend that it should be), ensure that there is a remedy identified in the SLA for such occurrences; i.e., for sluggish system response times or delayed throughput. Also, consider using third party tools to independently measure system performance (e.g. a content load ping test, application performance monitoring tools, etc.).

**Planned Downtime** - Also, service level metrics for system availability and performance items need to take into consideration the time periods allowed for planned maintenance windows known as “planned downtime.” The SLA should identify the service provider’s standard maintenance and release windows.

The difference between planned downtime and unplanned downtime is whether or not the service provider properly notified your organization in advance. Typically, planned downtime includes the service provider’s regular maintenance windows and any other downtime where they provide specified advance notification of any other maintenance windows that would take the system offline for a predetermined period of time.

The SLA should clearly state the advance notification required. Negotiate at least 48 hours' advance notice for unplanned maintenance where possible. Therefore, if the service provider does not notify your organization within 48 hours of taking the system offline, such downtime will count against their system availability service level.

**Clear Calculations** - When creating the calculations for system availability and performance metrics, follow these tips to establish clear metrics:

1. Express the acceptance standard as a percentage of uptime.
2. Show the full calculation of the specified percentage.
3. State both the percentage of uptime and the allowable unplanned downtime

**Rolling Time Periods** - Finally, the calculation agreed upon for the system availability should be based upon a rolling time period and not a calendar period. Therefore, if the system was not available on the last day of May and also the first day of June, both downtime periods would count against the total allowable downtime for a rolling time period.

**End Consumer Requirements** - When determining the acceptable standard for downtime that your organization is willing to accept, it is critical to fully understand and document requirements for system availability based upon a detailed analysis of the end consumer's needs. Costs can escalate dramatically with higher availability requirements. Therefore, contractually commit the service provider to a system availability and performance level standard for only what your end consumer really needs.

**Technical Constraints** - Understand the technical constraints between your organization and the service provider for being able to fully meet the end consumer's system availability and performance needs. For example, inform the end consumer that a certain degree of network latency is inevitable and that overall system availability may be constrained by system characteristics (e.g. custom configurations or running large reports can have a negative impact on system performance). Also, inform the end consumer that some planned downtime is required. Informing the end consumer of these items upfront will help to avoid unrealistic expectations.

**Monitoring and Automated Alerts** - A final consideration for system availability and performance service level monitoring is to ask the service provider if they use any monitoring tools that provide automated alerts for when the system goes down or is not performing at the acceptable standard of performance. It may be possible for the service provider to share these alerts directly with your organization.

## Cloud Specific Terms

As mentioned above, SLAs primarily exist in order to mitigate a service provider's risk profile back to the end consumer of their service, since the end consumer is relying on the service provider. In most cases, the end consumer is not entirely relying on the service provider as the only provider of that end-to-end service, or if they are, they can typically switch service providers without much disruption.

However, in the case of using a cloud service provider for either software as a service (SaaS), infrastructure as a service (IaaS) or platform as a service (PaaS), there is total dependence on the service provider and their ability to keep the service up and running without interruption. Due to this heightened risk profile providing maximum exposure to your service need, and potentially, to a critical process used by your organization, it is even more important to ensure that service level terms are in place.

**Tie Residual Payments to Performance** - Using a service provider in the cloud places an emphasis on the need for regular enforcement of SLAs. Therefore, consider holding back a portion of the software licensing fee (usually paid upfront via an annual subscription) and tying the residual balance owed to the achievement of certain service levels. This will help keep the cloud provider in a steady state of continued motivation to meet your service levels. Keep in mind that any payment method needs to comply with the Financial Management Regulations and policies.

**Option to Opt-Out** - In order to enable the end consumer of a cloud provider to continue using an older version of the software or system once the cloud provider moves to a newer version, try to negotiate into the underlying agreement or SLA the right to be notified before all new functionality releases with a right to opt-out (at least for a time period until the end consumer becomes comfortable with the new functionality and has been provided the necessary time to train others on the new version).

## Additional Considerations

Two additional considerations when negotiating the overall terms of your SLA:

**Engaged Supplier Management Program** - This is not a section to include in an SLA, but having an engaged supplier management program can help manage the SLA by providing the following operational aspects:

- Dedicated person/team that works with the internal technical support team and provider to understand the ongoing working relationship.
- Fosters a two-way street mentality for a successful ongoing relationship.
- Drives to dispute and issue resolution quicker and knows the escalation path.
- Serves as the enforcer or the “bad cop” by handling the tough conversation with the provider and seeks remedies when owed.

**Material Breach and Termination for Chronic Failure of SLAs** - Include “material breach” language to allow for full termination for chronic failure to meet standards or multiple occurrences, such as this example that is applicable for cloud or application service providers: “If either one or both of the following occur within any rolling 30 calendar day period: (i) two or more consecutive unplanned downtime hours; or (ii) four or more cumulative unplanned downtime hours occur (the result of one or more service interruption incidents combined), Customer shall be allowed to immediately terminate the Agreement and any Order Forms with Provider, and shall not be liable for any future committed fees beyond the termination date.”

For example, it might be acceptable for a portal to be down for 30 minutes at a time every week within a rolling 30 calendar days (a combined downtime of two hours), but it might not be acceptable for the same portal to be down at any time for two consecutive hours. At the same time under this example, if the portal was down for 60 minutes every week within a rolling 30 calendar days (a combined downtime of four hours), it would fail the service level.

- Down for two consecutive hours = Fail under the first service level specified.
- Down for a total of two hours, but as a result of four different incidents (each 30 minutes of downtime) = Acceptable.
- Down for a total of four hours, but as a result of four different incidents (each 60 minutes of downtime) = Fail under the second service level specified.
- Down for a total of four hours, but as a result of three different incidents (one for a consecutive of two hours, and two others each having 60 minutes of downtime) = Fail under both service levels.

Provided it is consistent with the Government dispute resolution process, the concept of immediate termination for material breach can also be used if critical bugs in coding cannot be fixed.

## Conclusion

Having either a standalone SLA or adding service level terms to your existing services agreement creates additional contractual protections thereby mitigating the overall risk profile of using a service provider. SLAs also provide a clearer path for seeking remedies in the event that service levels are not met.

When contracting for services, remember to ask the service provider to explain how each service component will be delivered to your organization and what constitutes acceptable standards for each measurable service item. Ensure the answers to all of your investigative efforts regarding service levels are incorporated into the underlying contract that governs the relationship for those applicable services.

Final thought: An SLA is like a mobile phone these days where you do not leave home without one; do not enter into a service provider relationship without having clear service levels, ideally articulated in a standalone SLA that your end users, technical team, supplier manager, legal teams, etc. can easily pick up, read, and use if needed. Give your teams the best starting position out of the gate; do not sign a contract without an SLA.

**About the Author**

Gretchen Kwashnik currently serves as Category Lead in Technology Supplier Management at Capital One in Wilmington, DE. Her responsibilities include technology acquisition, contract negotiations, and supplier management. Gretchen began her career at ING DIRECT in the Procurement department, drafting and negotiating IT and Marketing contracts. In 2008, she transitioned to the IT department, where she has since concentrated on technology acquisition, the software development life cycle, and the facilitation of IT projects. Gretchen has a Bachelor of Science in International Business from King's College and a Juris Doctorate from Widener University Law School.



DoD ESI is an official  
Department of Defense initiative  
sponsored by the Department of Defense  
Chief Information Officer (DoD CIO).

**Your Preferred Source for  
IT Acquisition Across the DoD**

- BEST VALUE**
- EFFICIENT**
- LOW RISK**
- VOLUME DISCOUNTS**
- UNIFIED VOICE**

Visit DoD ESI online at [www.esi.mil](http://www.esi.mil)

Department of Defense Chief Information Officer  
6000 Pentagon  
Washington, DC 20350-6000