1. **What role does having a service level agreement (SLA) play for supporting internal projects and IT services?**

An internal Sevice level agreement (SLA) acts as an agreement between an organization's IT department and its internal users (customers). Its primary role is to introduce a stable structure with clear communication; and professionalize IT services. In other words, it documents who is responsible for what. This avoids the blames when an issue arrives, as it clearly documents exactly what the IT department will deliver and what the users are responsible for. The IT department's success metric is moved from a "best effort" model to a "results-based model", meaning that this agreement holds staff accountable for specific results instead of just "working hard". Metrics include uptime, response times, or simple logical actions within time like if there's a critical issue the customer support should respond within 2 hours, whereas normally within 24h. Additionally, this SLA saves hours of productivity, stress and confusion. This is done by spending time upfront to agree on mutual understanding, so situations when requirements aren't clear are avoided. Communication is improved, and as a consequence the work environment of the employees too.

2. **What role does having an SLA play in supporting external projects with consultants or third-party service providers.**

For external organizations, the SLA is a crucial legal protection and a productivity measure. As mentioned earlier, SLA is designed to protect the organization's financial and operational interests instead of the old cooperative internal agreements, which can get messy quickly. For external projects, SLA guarantees specific services (for example 99.999% uptime), ensuring that the company gets the value they paid for. Also, external SLAs include specific penalties for specific breaches of the agreement (financial credits, refunds), or bonuses for exceeding targets, motivating the vendor to work harder and more efficiently. This is why the vendor in some companies is required to pay upfront for litigation costs if their failure causes the client legal problems (which can happen after a ransomware attack for example). In a SLA, performance is monitored transparently, which usually are real-time dashboards which are checked by third-party, with regular assessments. Finally, quality assurance is also prioritized, where the vendor commits to specific certifications, training levels, response times, backups are always made in case of a disaster and with a plan B (a clear process when initial support doesn't resolve issues). An external SLA is about lawsuit protection and accountability across organizations.

3. **Suppose you have been tasked with overseeing a service level agreement with another company that can provide backup services to the 500 PC users of your company. Use the Internet to research and develop a set of metrics that could be used to assess service availability, quality standards, and security to be part of an SLA.**

A. Service Availability Metrics

1. System Uptime (the “five-nines”). Depending on the type of company, this can have 2 values: 99.9% uptime (meaning 8.7 hours of downtime are allowed per year), and this would be for non-critical data or 99.99% uptime (52 minutes of downtime per year) which is mainly used by active businesses.
2. Scheduled maintenance shall not exceed 4 hours per month.
3. Time to initiate a file restore request must not exceed 2 seconds. This is known as access latency.
4. 24/7 access to backup services in case of any situation.
5. If a maintenance is planned, it must be announced 7 days in advance.

B. Quality Assurance Metrics

1. 99.5% of all scheduled user backups must complete without error. Anything below this puts too much data risk.

2. Next is RPO (Recovery Point Objective). This means how much data can be afforded to be lost. As standard approach would be to do backups every 24h, but for more scalable and high performance systems it must be done every 4 hours.

3. RTO (Recovery Time Objective) is how fast can data can be get back. Critical file restoration must be at most 2-4 hours.

4. 99.9% of backed-up files must be restorable (integrity check). Vendors should run automated "test restores" to prove files aren't corrupted and avoid hazardous situations.

5. Restoration speed must be at a minimum 10 MB/second download speed.

6. Deleted files must be kept for at least 90 days and 1 year for critical business data to avoid it being necessary in the future.

C. Security Metrics

1. Data must be encrypted using reliable encryption methods that haven’t been cracked. An example of a metric would be this: “All data must be encrypted using AES-256.”

2. In case of a security breach discovered by a vendor, the vendor must notify the client within 24 hours of discovery.

3. Critical security patches must be applied to vendor servers within 48 hours of release.

4. Multi-factor authentication (MFA) required for all user accounts. After 5 attempts, 30-minute lockout period.15 minutes of session activity for web, relogging required.

5. 100% of administrative actions logged and retained for 2 years for transparency and no abuse.

6. 100% of data must be stored within the client’s country’s data centers to comply with local regulations.

7. Daily automatic updates for anti-malware/antivirus software.

8. GDPR compliance.

These metrics really depend on the type of customer you’re serving. They assume the company is a standard company and not a premium company.