

Negotiating Effective Vendor Contracts & Service-Level Agreements

Overview:

- **Contracts vs. Service-Level Agreements**
- **Contracts**
 - 3 Phases of Negotiation
 - Regulatory Requirements
 - Pricing & Terms: What to Look For
- **Service-Level Agreements**
 - 4 Steps to a Stellar SLA
 - Measuring & Monitoring Vendors




Vendor Contracts vs. SLAs

Contracts

Contracts define the business relationship between a financial institution and a vendor by outlining key terms and provisions, including costs, key dates, risk controls, remedies, and termination processes, among others.

SLAs

SLAs are an element of a vendor contract that specifies performance standards and establishes benchmarks for service.



SECTION ONE

Contracts

3 Phases of Contract Negotiation



Assessment Phase:

1. Assess Your Needs

2. Assess the Market

3. Define the Costs

Assess Your Needs

- Define your business need
- Identify desired features
- Ensure goal alignment
- Assess third-party risk
- Risk mitigation

Assessment Phase:

1. Assess Your Needs

2. Assess the Market

3. Define the Costs

Assess the Market

- Seek referrals from:
 - Peers
 - Professional associations
 - Favorite vendors
- Develop a vendor short list
- Focus on what makes each vendor stand out

Assessment Phase:

1. Assess Your Needs

2. Assess the Market

3. Define the Costs

Define the Costs

- Direct costs:
 - One-time fees
 - Fee increases
 - Termination fees
- Indirect costs:
 - Training
 - Management oversight
 - Compliance

Planning Phase

Benchmarking

- Determine market pricing
- Ask around
- Not easy to compare
- Focus on the overall cost

Negotiation Phase



Pricing



Terms

A Note on Timing

- Track key contract expiration & auto-renewal dates
- Effective negotiation requires a strong needs assessment
- Begin assessments long before expiration date

Understanding “Discounts”

- Flex credits
- Line-item invoices

Strategies for the Best Pricing

- Compare vendors directly
- Leverage the competition
- Seek out incentives
- Align interests

SECTION TWO

Terms

Regulatory Expectations for Contracts

1. Nature and Scope of Agreement
2. Performance Measures or Benchmarks (SLA)
3. Responsibilities for Providing, Receiving & Retaining Information
4. The Right to Audit and Require Remediation
5. Responsibility for Compliance With Applicable & Regulations
6. Costs and Compensation
7. Ownership and License
8. Confidentiality & Integrity
9. Operational Resilience & Business Continuity
10. Indemnification & Limits on Liability
11. Insurance
12. Dispute Resolution
13. Customer Complaints
14. Subcontracting
15. Foreign-Based Third Parties
16. Default and Termination
17. Regulatory Supervision

What's Missing?

48% No business continuity plan requirement

27% No incident response requirement

80% No performance standards

14% No data security and confidentiality requirements

44% No audit or reporting requirements



Nature & Scope of Agreement

Meaning:

What does the vendor provide in service, support & software?

Potential Issues:

Could someone who has never seen the solution (a regulator) understand the purpose of the agreement by only reading the agreement?

Mitigation:

Details describing why you have this service, software, and/or support.

Nature & Scope of Agreement

Meaning:

Who owns the data?
Where is it hosted?
What levels of security
are in place?
Who tests the security?

Potential Issues:

Data ownership is key.
Should have IT security
provisions.
If there is a dispute or
issue, how does the
financial institution
continue to deliver
service to the customer?

Mitigation:

Details of IT security.
Details showing the
financial institution
owns its data.

SECTION THREE

Service-Level Agreements (SLAs)

Service-Level Agreements

An SLA is a document that:

1. Describes the level of service expected by a customer from a supplier
2. Lays out the metrics for measuring service
3. Lists the remedies or penalties should the agreed-upon level of service not be achieved

4 Steps to a Stellar SLA



Determine Priorities



Choose What to Measure



Define Specific Criteria



Set Enforceable Consequences

Determine Priorities

Identify the most critical
performance and risk factors

- Availability and timeliness of service
- Data confidentiality and integrity
- Change control
- Security standards
- Business continuity
- Help desk support

SECTION FOUR

Choosing What to Measure

A hypothetical exercise

What's Measured?

Accurately and objectively measuring performance

Performance metrics should:

- Be defined by your institution
- Reflect your institution's unique needs
- Be specific to your institution and not an "aggregate" of all the vendor's customers
- Cover specific periods of measurement.

Who Does the Measuring?

The short answer is you.

Retain control of how measurements are made:

- Don't let the vendor pick the measurements.
- Don't leave the vendor in charge of measuring.
- Require that vendors give you monitoring tools and reports
- Controlling this yardstick helps ensure you'll be compensated in the event your vendor falls short

SECTION FIVE

Defining Specific Criteria

Define Terms

1. Timely notification
2. Unauthorized access
3. Security incident
4. Substantial harm or inconvenience
5. Potential breach
6. Significant disruption
7. Material impact
8. Cyber event
9. Uptime
10. Critical failure
11. Uptime

SMART Metrics:

Specific
Measurable
Achievable
Relevant
Time-bound

Specific: Availability of Timeliness and Service

- Speed to go from Point A to Point B when clicking a link
- Speed of web-based platform loading
- Speed of report loading
- Processing times
- Item posting timelines
- Posting accuracy
- Allowable error rate
- Customer service response times

Specific (Cont.)

Confidentiality & Data Integrity

- Monitoring
- Performance of penetration testing

Change Control

- Define “change”
- Set standards for the change process (processes & procedures)
- Define roles & responsibilities

Specific (Cont.)

Security Standards Compliance

- Include monitoring of security
- Require third-party verification of standards & measurements

Business Continuity

- Recovery time objectives (RTOs)
- Recovery point objectives (RPOs)
- Record retention
- Data protection
- Maintenance/testing of BCP & disaster recovery plans

Specific (Cont.)

Customer Support

- Define customer support (i.e. delivery method)
- Hours of availability
- Escalation procedures

Special Note:

Include periodic review & change provisions to ensure that service level goals and performance measurements can evolve with business and technology needs.

SECTION SIX

Enforceable Consequences

If you look at many standard SLAs, the only consequence for falling short of SLA benchmarks is that the vendor redoes its work – something it must do anyway.

Financial Penalties

What's Reasonable?

- A small percentage off the service fee during the period of underperformance
- Not meant to be a profit center
- Escalation clauses to increase the amount if there are continued violations

Example: 3% discount during measurement period if mission critical service goes down

- Be careful what performance you incentivize
- High processing speed or volume isn't good if it's not accurate



Termination

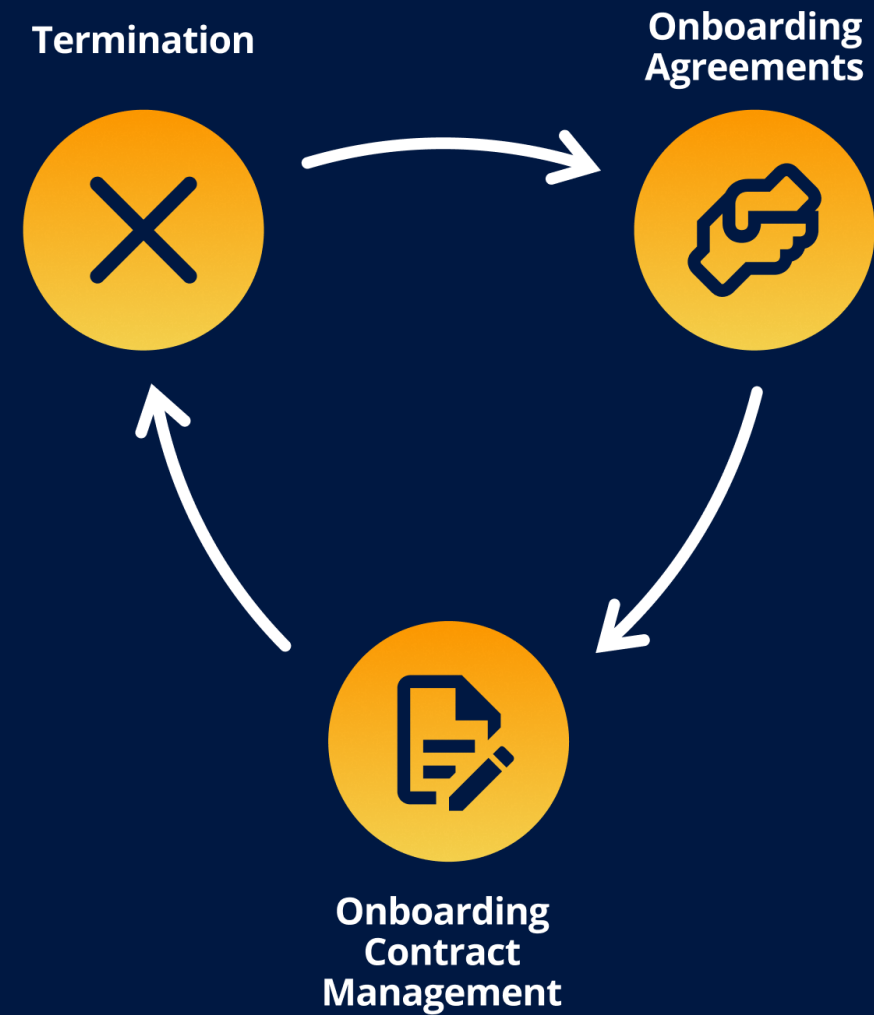
What's Reasonable?

- Provide specific path and timeframe to correct mistakes
- Termination provisions defining contract default
- Termination is a last resort

SECTION SEVEN

Contract Management

Contract Management Lifecycle



SLA Monitoring



- If you're not following up and monitoring vendor performance, your SLA has limited value.
- Monitoring is an essential part of your vendor management program.

Takeaways:

- Contracts are negotiable – but you need to know what to ask
- Know what you want going in
- Compare contract drafts to regulatory requirements
- Pay attention to the details
- Take note of key dates and pricing
- Integrate contract management & vendor management program

 **CONTRACTS**

Thank You.