Technology Agreements
For the Non-Techie Attorney

Presented by

Matthew Stippich
General Counsel, Digital Intelligence
Partner, Stippich Selin & Cain sc
mstippich@digitalintelligence.com

Alan Kesner, City Attorney
City of Wauwatosa
Wauwatosa, WI 53213
akesner@wauwatosa.net

2017 Wisconsin Municipal Attorneys Institute

JUNE 14, 2017

I. INTRODUCTION:

A. Types of Technology Agreements

1. <u>Traditional Software Licensing (off the shelf</u>*)*. The traditional software license is typically installed on a local machine or "on-premises".

a) ***Advantages***:

(1) **No ongoing fees (except. . . .).** Once installed, perpetual licenses can be used forever.

(2) **Bug Fixes for period of time**. Most off the shelf software includes the ability to patch or update the version of the software for a period of time.

b) ***Challenges***

(1) **Support**. Support, if provided, is typically provided under a separate fee agreement, thus making the license very similar to a subscription license.

(2) **Infrastructure**. You will have additional infrastructure to purchase, configure and maintain for proper operation of the license. Traditionally much of IT staff time has been devoted to the maintenance of the infrastructure rather than the applications.

2. <u>Custom Software Development</u>. Custom software development agreements are less common in a municipal environment.

a) ***Advantages***:

(1) **Custom Software**. When developed in accordance with a specifications document, a custom application is like purchasing a custom suit. It fits perfect and fulfills all requirements.

b) ***Challenges***:

(1) **Support**. Ongoing support can be a challenge when a custom software application does not have a broad user base. The developer does not typically maintain a schedule of updates or improvements. You are essentially fixed in time with the functionality that you have purchased until you pay to create improvements to the software. It is also very difficult to switch from one vendor to another with custom software.

(2) **Security**. One of the biggest challenges with legacy or custom software applications is the vulnerability to security

flaws. SaaS applications are more easily patched or updated to address concerns.

3. <u>Software as a Service (SaaS)</u>. SaaS computing involves the remote hosting of a software application. Google Docs, Office365, Yahoo! Mail and Survey Monkey are all examples of SaaS offerings.

a) *Advantages*:

(1) **Minimal local infrastructure**. An end user typically will only need a web browser or a local thin-client to access the SaaS application. A basic computer and an Internet connection is usually sufficient.

(2) **Generally available anywhere, on-demand**. Both SaaS and cloud computing are offered on subscription basis and can be accessed instantly – from anywhere a user has an Internet connection.

(3) **Frequent, seamless update of features**. Because of the centralized structure of a SaaS application, service providers can create and implement bug-fixes or improvements instantaneously.

(4) **Change in IT staff focus**. As a result, the IT staff won't need to occupy your computer every 6 months to update your software or make sure you have the latest patch for a certain application. All of those maintenance issues are taken care of on the "server side".

b) *Challenges*

(1) **Control of Data**. For better or worse, data is not stored locally. This can be beneficial in disaster recovery situations, but it does raise issues of security and restrictions on access by third-parties. This can also be an issue when you are required (through open-record or litigation request) to search and produce documents.

(2) **Pricing**. Once you are tied in to a subscription, it can often be difficult to move to another system, thus giving the vendor pricing leverage.

(3) **Security**. The end user has limited control over the security of its data. The benefit is that your local IT department has less obligation to maintain a secure infrastructure. Security provisions should be reviewed closely and special attention should be given to critical data

(employee data, end user PII or PHI, financial data, privileged data, trade secret data, etc.).

II. THE TECHNOLOGY LIFECYCLE

A. The Technology Lifecycle (pre-cloud / SaaS)

1. <u>Assessment/scope (establish thresholds).</u>

a) ***Determination of the financial institution goals/objectives***. What type of service is desired? What technology tools can be used to assist with the process? Is this a critical business function? Is this a business function that has a cost component that can be shared with the Licensee?

b) ***Analysis of core competencies***. Often, an organization will thrive when it sheds those aspects of its operation that have not reached critical mass.

c) ***Cost/benefit analysis (total cost) of internal/external operation***. It is **critical** that an organization fully consider the total cost of ownership related to a particular licensing or outsourcing model. Often, a vendor will present savings calculations that do not consider costs related to administrative responsibilities, organizational paradigm restructuring, and personnel costs.

2. <u>Request for Proposal</u>. A full-blown RFP process is not necessary (nor recommended) for all situations. However, the process of developing an RFP questionnaire often assists the enterprise in establishing the functional requirements that will be expected from a vendor. Focus on those items that are critical to the relationship (include base-line legal and performance terms), and avoid a laundry list RFP. Remember, as a Licensee, you have the greatest leverage regarding essential terms and conditions when multiple vendors are involved. If an RFP is used, indicate that the response will be used as a basis to develop performance warranties and standards under any ultimate agreement.

3. <u>Pre-Negotiation Analysis</u>. To select a vendor objectively and adequately assess the total cost of ownership, it is important to receive input from non-user decision makers. A common mistake occurs when the end-user is allowed to review and select the vendor solely on a perceived deliverable without having any context for the financial and legal concerns. In this situation, it becomes virtually impossible to negotiate pricing concessions or changes in the legal allocation of risk. Therefore, prior to the selection process, you should involve the following:

a) ***Technical review***. Your technical team should provide information regarding the cost of owning/outsourcing a particular technology. What additional employees will be needed? Will interfaces or customization be required for any current technology? Once you are committed to a technology or outsource relationship,

how difficult is it to change vendors? Are you considering "industry standard" technology?

b) ***Legal review***. Your legal team should provide an analysis of risks, threats, exit strategies, and remedies balanced with sound business judgment. Every legal decision has business implications, and every business decision has legal implications. Typically, your attorney should have substantial experience in reviewing and commenting on similar deals.

c) ***Financial review***. What is the total cost of implementing the technology? How is this expense measured on a per consumer transaction basis? Can this expense be shifted to an end user? What is the return on investment in the form of cost savings, increased efficiencies, or competitive advantage?

4. Selection.

5. Final Negotiation. The final negotiation process should focus on those factors that are critical to the particular outsourced application. Consideration should be given to those specific provisions set forth below. The most important provision of any outsourcing agreement involves those remedies available to the Licensee in the event of non- or substandard-performance by vendor.

6. Management (audit, renewal, termination). Upon signature of a definitive outsourcing agreement, the most critical process has just begun. Failure to vigilantly monitor and manage an outsourced relationship is a recipe for disaster. Often, the remedies offered a Licensee under an outsourcing arrangement are only triggered upon notification from the Licensee.

B. Lifecycle (post Cloud/SaaS)

1. End user selection. Today, end user selection drives a vast majority of technology "contracts" entered into by organizations. Traditional software licenses, SaaS arrangements and cloud options are all readily available through basic Internet access, thus allowing users to commit to terms with the click of a button.

III. KEY PROVISIONS

CAUTION: Any sample provisions in this outline are provided for discussion purposes only and DO NOT represent preferential default language.

A. Definition of License / Service

1. License Term.

a) ***Perpetual Licenses*** provide the licensee with the ability to use the *licensed version* of the software in perpetuity. Most perpetual licenses do not include software updates or improvements.

b) ***Term Based License*** define a duration for which the user will be permitted to use the software license (on-premises software license) or otherwise have access to the software online (SaaS based license). Vendors typically want to secure a term commitment rather than pay-as-you-go and will utilize pricing incentives to encourage the commitment. (see section on Termination Penalties).

2. License Grant. All software license agreements or technology service agreements involve the grant of a license to access or use certain intellectual property of the vendor. A typical license grant would be as follows:

Sample generic license

x. Grant of License. Subject to the terms and conditions of the Agreement, Vendor grants to Licensee a non-exclusive, non-transferable license to use the software identified in Exhibit A (the "Licensed Programs") for the purpose of xxxxxxxxxxxxxxxxxxxxxxx. Licensee may use the Licensed Programs in executable format for its own use.

3. User Limitations. Many software and most SaaS licenses will limit the number of users who can "use" or "access" the software or the information contained in the online service. The following is a sample clause:

Sample License to Limited Users

x. Grant of License. (a) Subject to this Agreement, Vendor grants and Licensee accepts a non-exclusive, non-transferable license to Use, in the Territory, the Software, Documentation, Third-Party Database, and other Vendor Proprietary Information provided by Vendor to Licensee, at specified Designated Site(s) within the Territory for Productive and Non-Productive Uses.

Any individuals accessing the Software on behalf of Licensee, its Affiliates or Business Third Parties must be licensed as Named Users. The maximum number of Named Users (or other relevant metric) licensed to access the Software, and/or Third Party Database, shall be specified in Appendices to this Agreement.

NOTE: User limitations should be carefully reviewed in the context of a SaaS agreement. To the extent web based users will have access to information or reports generated from a system, those potential "users" should be excluded or defined carefully.

B. Pricing

1. Price protection (MFC). The best time to negotiate pricing is BEFORE you have selected a vendor. A common mistake is to choose a vendor and then negotiate price. Many SaaS based applications are subscription based and Vendors prefer a significant term commitment with termination penalties for not completing a term. Consider including a MFC clause to ensure price protection:

> ***x. Most Favored Customer.*** Vendor warrants that the prices charged for the Services under this Agreement are the lowest prices charged by Vendor to any of its external customers for similar volumes of similar Services. If Vendor charges any external customer a lower price for a similar volume of similar Services, Supplier must notify Licensee and apply that price to all Services ordered under this Agreement. If Vendor fails to meet the lower price Licensee, at its option, may terminate the balance of the Agreement without liability.

2. Consider partial licenses. Some vendors will permit limited access licenses for users that do not use the full functionality of the software/service. For example, a user may only have the need to access the system for informational queries. Consider negotiating limited access licenses to address this limited functionality.

3. Do not agree to early termination fees. If you are unable to remove the early termination fees completely, consider including a clause that caps the fee at the license level for the actual services delivered. For example, if you receive a 10% discount for agreeing to a 5 year term vs. a 2 year term and you terminate at the end of 2 years, the termination fee would be limited to the discount you would have not otherwise received (24 months at 10%).

C. Performance / Availability

1. Latency. Latency involves the end-user experience. How long does it take for the end-user to get data when a request is made from their computer.

2. Up-Time / Availability. Availability refers to whether the application is available to the end-user. Many availability clauses include a 9x.xx% uptime guarantee. Rather than agree to this blanket availability standard, it is best to carve out a higher standard for "normal business hours". 98% uptime could mean 2 full "work days" of downtime in a given month. This would be unacceptable. If those 2 days fall on a weekend, it will have a different effect on the organization.

3. Caution on use of Non-Performance Credits. A vendor will often include a "credit" clause to enumerate a remedy for non-performance. Often this remedy is completely insufficient to offset the "damage" you endure for the performance failure.

> ***x. Service Interruption.*** Licensee will be given a service credit for interruption in excess of thirty (30) minutes as measured from the time of notice by Licensee to Vendor until the time the service is restored. **{Caution: Consider WHEN interruption measurement event starts. In this example, Licensee must notify the vendor.}** In such an event, Licensee shall be entitled to only those service credits calculated as follows: (number of 30 minute periods of interruption / 1440) x monthly recurring charges for each affected circuit. **{Caution: This example uses a multiple times the "affected" circuit. A Vendor will often try to limit credits by including credits only for limited items. If the entire service or system is affected, however, the appropriate credit should be adjusted.}**

4. Tie to termination

> ***x. Termination for Interruption of Service.*** If Customer experiences a material and repeated interruption of service in a given location, including the failure of Vendor to achieve the service level commitments contained in any Service Level Commitment Addendum, Customer may, by giving written notice thereof to Vendor, (i) terminate service for the affected equipment or services affected by the service interruption as of the date of receipt by Vendor of such notice, or as of a future date specified in such notice of termination; or (ii) terminate this Agreement and any services. No termination fee pursuant to Section xx shall be chargeable with respect to such terminated services and Customer's discount will not be reduced if service for affected equipment or service is terminated under this Section.

D. Data/Network Security

1. Network Access Clause. Given the connected nature of today's SaaS applications, it is critical that you consider restrictions on a Vendor's access to your network. The purpose of this clause is to clearly define when access will be permitted, and by what means.

> ***x. Vendor Access.*** Vendor must contact Licensee's Security Department prior to entering Licensee's premises or accessing Licensee's computer network or equipment. If Vendor will have access to Licensee's computer network, or any of Licensee's computer equipment, Licensee may provide Vendor with a password or other unique access code for access to

such equipment. Vendor assumes all responsibility and liability for the use, protection and confidentiality of the password or access code. Vendor agrees to immediately notify Licensee if the confidential nature of the password is compromised, or if Vendor become aware of any loss, theft, or unauthorized use of the password or access code. Any access permitted by the Agreement is expressly limited to such access necessary to perform the services or delivery the product provided in the Agreement. If Vendor will access Licensee's computer equipment remotely, Vendor represents and warrants that all access by Vendor will be via a connection that utilizes the minimum industry standard Secure Socket Layer (SSL) encryption or a comparable encryption technology to protect the security of the information received by, or transmitted from Licensee.

2. Disabling Code Clause. A clear disabling code clause relates to affirmative obligations of the vendor to make sure the application does not contain any virus. The following clause also contains language to prevent vendor "self-help" remedies, like disabling the software while a dispute is in process.

> ***x. Disabling Code Warranty.*** Vendor warrants and represents that no product or service provided to Licensee pursuant to the Agreement will contain, and Licensee will not receive from any Vendor data transmission via modem, the Internet or other medium, any virus, worm, trap door, back door, timer, clock, counter or other limiting routine that would erase data or programming or otherwise cause any software, system or equipment to become inoperable or incapable of ordinary use (a "Disabling Code") including, without limitation, any limitations that are triggered by: (a) any software being used or copied a certain number of times, or after the lapse of a certain period of time; (b) any software being installed on or moved to a central processing unit or system that has a serial number, model number or other identification different from the central processing unit or system on which the Software originally was installed; or (c) the occurrence or lapse of any similar triggering factor or event. In the event Vendor introduces a Disabling Code into any of Licensee's equipment, at no additional cost to Licensee, Vendor shall: (a) furnish Licensee with replacement product or services without the presence of Disabling Codes; (b) install and implement such new product or services; and (c) take all steps necessary to restore any and all data or programming lost by Vendor as a result of such Disabling Code. Notwithstanding the foregoing, Vendor and Licensee understand and acknowledge that any code included in the licensed Software that prohibits use outside of the license scope purchased for the Software shall

not be deemed to be "Disabling Code". If a Disabling Code is triggered for any permitted use within the license scope purchased for the Software, Vendor, within twenty-four (24) hours of receipt of notice from Licensee, shall be required to restore the Software to its original operating condition and shall be liable to Licensee for any actual damages incurred as a result of the Disabling Code.

E. Data Ownership. Clear data ownership is critical to providing flexability to any SaaS arrangement. You should make clear that the data (and any data created by the system) is owned by you. You should also make sure you have a method for extracting the data from the system periodically and in the event of termination.

x. Ownership of Data. Licensee shall maintain ownership of all data entered into the System and any and all data compilations created as a result of using the System. All Licensee data entered into the System will be maintained in an isolated access controlled data domain and cannot comingle with other Licensee data. Personal identifying information and any medical information will be adequately secured at rest and in transmission. Licensee, at no cost to Licensee, may download or obtain a full and complete copy of all data in the System at any time during the term of this Agreement.

y. Data Transfer Upon Termination. Upon termination or expiration of this Agreement, Vendor will provide one electronic copy of Licensee's data in ASCII, text-delineated format on optical disk (compact or digital versatile) upon request. Other data formats requested by Licensee may be provided by Vendor at Vendor's sole discretion. Vendor reserves the right to erase or remove any data stored in Vendor's facilities after providing Licensee with the aforementioned data file(s), provided Vendor gives Licensee at least ninety (90) days advance written notice. Vendor will also wipe clean and erase any and all data upon the written request of Licensee, and will certify and represent to the complete deletion thereof.

IV. SELECT OUTSOURCING CHALLENGES

A. *Outsourcing Challenges*. To adequately negotiate an outsourcing relationship, you must first understand the characteristics of an outsourcing relationship and the challenges created. Outsourcing arrangements present four key challenges, which if not addressed, introduce significant risks for the financial institution. While other risks exist, the primary concerns are:

1. Selecting a qualified vendor and structuring the outsourcing arrangement – Failure to choose a qualified and compatible service provider, and to structure an appropriate outsourcing relationship, may

lead to on-going operational problems or even a severe business disruption. These events may result from service provider employees not having the necessary skills or familiarity with the industry, or from service providers lacking an adequate technical capacity or financial stability.

2. Managing and monitoring the outsourcing arrangement – As management focus shifts from direct to indirect operational control over an activity, there is a risk that undue reliance may be placed upon the service provider by the financial institution. Without active management and monitoring of the relationship, sub-par service may occur or, at the extreme, loss of control over the outsourced activity. Given the customized nature of service contracts, changing service providers in the face of unsatisfactory responsiveness may not be a viable option. Even when alternatives are available, switching service providers is likely to be a costly option that adds to operational, legal and other risks.

3. Ensuring effective controls and independent validation – Given the reliance on a third party for the performance of critical activities, there is the risk that without independent validation of the control environment the institution cannot determine that the controls have been effectively implemented. The service provider also may not always maintain the necessary capacity, employee skill set or financial capability as agreed to in the contract.

4. Ensuring viable contingency planning – Given the dependency on a third-party service provider, financial institutions face the challenge of ensuring adequate contingency planning to avoid business disruptions. What contingency plans does the service provider have in place? What contingency plans does the financial institution have in the event of nonperformance by the service provider? Recurring performance problems coupled with the absence of comprehensive contingency plans by the service provider and the financial institution may result in unintended credit exposures, financial losses, missed business opportunities and reputational concerns.

V. NEGOTIATION TIPS

A. There are as many negotiation strategies as there are agreements to be negotiated. We recommend having more than one person involved in the negotiation process. As we have indicated above, an end-user is often biased and becomes a proponent of the vendor and salesperson. Use a purchasing agent or attorney to play the appropriate "bad cop" role. Regardless of your method of negotiation, never tell a vendor the following:

B. ***Never Tell A Vendor . . .***

1. your budget

2. they are a "strategic partner"

3. you have a deadline
4. you love their product
5. names of others involved in the acquisition unless it will work to your advantage
6. who their competition is
7. the bids you received from other vendors
8. who won the bid
9. they are the only ones being considered (even if they are)
10. your profit margins
11. you need their product
12. you prefer their product over the competition
13. their price is reasonable

VI. SELECT TECHNOLOGY CONTRACTING ISSUES

A. ***Understand your objectives***. The most frequent cause of unsuccessful arrangements is that the service provider did not meet management's expectations - usually because these expectations were poorly understood or articulated by both parties involved. Such a situation may arise in IT outsourcing, for example, because end-users may not be sure of their needs, the technology may be new or untested, business requirements change frequently, or implementation did not occur as expected. In some situations, senior management may have conflicting objectives for the arrangement, or unrealistic expectations as to what problems the outsourcing can solve. For example, if outsourcing is undertaken primarily to reduce costs or to convert fixed costs to variable costs, it may result in an arrangement that compromises quality, timeliness and level of service, which may be unanticipated by management and lead to disappointment with the arrangement. In such cases, as the situation deteriorates, outsourcing risk increases.

B. ***Key elements of the contract include:***

1. **Scope of services**. What specifically is to be outsourced.

2. **Performance Standards/Functional Specifications**. Engagements for custom software or technology should include a statement regarding functional specifications. It is important to include explicit expectations regarding integration with existing systems, compliance with regulatory requirements, and performance standards. Payment milestones, warranty provisions and maintenance standards should be in relation to specifications.

3. Pricing. An outsourcing agreement will often include several levels of pricing – implementation/conversion, up-front "license" fees, hardware costs, and support and maintenance.

a) *Implementation Pricing*. Often an outsourcing agreement will include fees associated with implementation or conversion of a technology. While it may be necessary to provide an up-front payment for the conversion, it is important to retain a substantial amount of payment until a "go-live" status has been achieved.

b) *Customization*. If the vendor includes or contemplates custom software and interfaces written specifically for the Licensee, the Agreement should clearly define what will be received, who will pay for the customization, who owns the interfaces, and who will maintain the interfaces. ***TIP:*** Often, a vendor will insist that the Licensee pay for custom interfaces for standard applications (PeopleSoft, MySAP, Fiserv, etc.). Once the interfaces are developed, the vendor will want to use the interfaces with other Licensees. The financial institution should ensure that it does not pay for development of core vendor modules. Maintenance provisions should also be modified to ensure continued support of customizations.

c) *Ongoing maintenance/Service Fee*. A Licensee must aggressively negotiate the pricing model for the transaction. Vendors will try to use a model that maximizes their revenue, often based on a metric that does not accurately measure "use" or "cost of service". For example, many vendors in the ERP business have sought per transaction charges which often result in fees that exceed "traditional" pricing models. Another "trick" involves charging for indirect use of the outsourced service, such as with a system that provides an e-commerce interface to Licensees.

d) *Incentives*. Contracts may offer bonuses for exceptional performance and penalties for poor performance. Overall, they should be used to align the interests of the service provider with that of the financial institution

e) *Pricing level*. Negotiate most favored pricing terms based on usage and volume.

f) *Termination penalties*. If possible remove any termination penalties (to Licensee) for termination of the agreement. The only time termination penalties are justified is when the vendor has made a capital investment in the outsourced services that must be recouped over the life of the agreement.

g) *Audit ability*. The right to conduct audits of the service provider and/or accept third party reviews of their operations

4. Retained ownership and confidentiality of data shared with service provider.

5. Warranty Provisions. Warranty provisions should include a compliance with law statement. Depending on the leverage of the Licensee, you may want to negotiate an ongoing maintenance/warranty provision to ensure compliance with future regulatory changes. If a vendor is unwilling to warrant and provide updates, you may consider an alternative remedy that allows you to terminate the relationship (license and maintenance). ***NOTE:*** Including third-party software products in the definition of the product the financial institution is purchasing from the vendor is essential to ensure that the vendor is responsible for third-party software *to the same extent* that the vendor is responsible for its own software. The vendor is in the best position to evaluate the third-party software in relation to the vendor's system. The financial institution should not be placed in the position of having to determine which component of the system caused an error and which party should be held accountable. Without such a provision, the vendor and the third party may blame each other for any implementation failures, causing delays and cost overruns, as well as preventing the financial institution from holding either party accountable for the problem.

6. Business Expansion/Down-turn Provisions. Another issue associated with the definition of products is the ability to acquire additional products from the vendor at a favorable price. The pricing terms obtained during initial contract negotiation are likely to be the most favorable, as that is when the financial institution's bargaining position is the strongest. To ensure that the financial institution will continue to receive favorable pricing, and to keep costs down, agreements should include a provision for the optional acquisition of additional products in the same (or a related) product line at a specified price or discount from the published list price. Once acquired, those additional products should become part of the definition of the product that is licensed, warranted, and supported under the agreement. For contracts based on usage, you should also include provisions that allow the Licensee to reduce volume based on a business downturn. This may result in higher per-item fees, but should reduce the overall cost of the outsourcing arrangement.

7. Term/Termination. If the Vendor is providing a service without significant capital investment, a Licensee should push for unilateral ability to terminate without cause. In the alternative, a Licensee may want to negotiate a "change in technology" clause that provides the Licensee the ability to terminate the agreement in the event a new/different/better method of performing the task is discovered.

8. Non-termination remedies. Often, a vendor will offer two remedies for a failure to meet performance requirements: i) service credits and ii) termination. Neither of these remedies provides you with the desired result – a product/service that works. Service credits can provide an "incentive" if they are structured with enough impact. However, you will

occasionally find a situation where the vendor simply is incapable or unwilling to correct the problem in a timely manner. Therefore, you should also consider ***self help remedies***. One example allows you to seek an alternative vendor to correct a defect in performance and bill the charges back to the vendor.

C. ***Maintenance and Support***.

1. Service Level Agreements (SLA) should provide the following:

a) Minimum maintenance obligations of vendor during term.

b) General description of maintenance services.

c) Program corrections and "fixes."

d) Response times for critical and non-critical problems.

e) Enhancements (cross-reference to "Software Enhancements").

f) Type of media provided.

g) Location of maintenance (e.g., on-site, vendor offices, telephone assistance).

h) Compatibility of maintenance fixes and other releases with original software and hardware

i) Maintenance availability warranty by vendor that maintenance will be available to user (at standard rates and terms or better) during entire term or other specified minimum period after acceptance, and reasonable notice period.

j) Allowance or credit in event of operational failure in excess of specified limits during license term or during a specified period following acceptance.

k) Methods of determining failure, calculating allowance, and notifying vendor.

l) Eliminate risk that any credits or liquidated damages will be deemed to be user's exclusive remedy.

m) Reasonable limitations and conditions on any credit obligations of vendor. (Generally, limitations and conditions should exclude any credit factor caused by specified actions or inactions by the user or other third parties; however, such events should not reduce vendor liability for credits caused by other factors.)

n) Updates and New Releases. The financial institution should obtain a broad definition of "updates" and "new releases." For example, the financial institution may define new releases to include products that replace the licensed product. Such product replacement can often occur when the vendor is purchased by another software company, or switches to a different computer platform. At a minimum, the agreement should allow the financial institution to purchase the replacement product at the same terms as the original purchase. A broad definition of

updates should prevent the vendor from attempting to generate a continuous revenue stream by providing a series of minor changes to its software and classifying them as new releases, thus charging additional fees to the financial institution for the new product. Other provisions should address legal compliance, price, frequency, warranty periods for enhancements and compatibility warranty.

2. Remedial Action. The purpose of an SLA is to protect your company against the worst case. Effective SLAs do more than get a nominal credit back - usually 5% to 10% of the cost of the service in the event your infrastructure fails. When written properly, SLAs give you a way to mitigate the effect of problems that harm your network.

Licensing/Technology Agreement Checklist

License/Development Agreements.

- ***NOTE:*** The following list is not intended to be an exhaustive list of issues related to negotiating a license agreement, but rather a summary of common provisions and issues related to these provisions.

  - ***Grant of License***. Is the grant to use limited or perpetual? Does the scope of use satisfy your intended use (per CPU, per user, global, site, server, etc.)? May the license be transferred to a subsidiary? Upon sale?

  - ***Performance standards***. Does the agreement clearly spell out the vendor's obligations, timetables and deadlines for completion of daily, monthly, quarterly or annual functions? Does it provide other service standards and a mechanism to review and correct deficient service levels?

  - ***Work For Hire***. Will original work product be created? Does the agreement expressly state that all work done by the programmer/consultant is work for hire, and does the consultant/programmer expressly assign all rights in the work to you? Does the consultant retain any rights? May they utilize "residual" information? Do you require ownership? What about creation of a similar product for a competitor? If so they should be spelled out.

  - ***Delivery/Acceptance***. What is the timing for delivery? Is payment contingent on delivery? Configuration? Is there an acceptance procedure? What happens if the deliverables do not conform with specifications?

  - ***Payment Method***. Are milestone payments appropriate? Has a hold-back amount been established as an incentive? Have revenue-recognition issues been discussed? Fixed price? Hourly? Annual?

  - ***Originality/Noninfringement***. Does the programmer/consultant warrant that the work will be original or al least will not infringe any copyright, trade secret or other intellectual property right?

  - ***Regulatory compliance.*** If the software will be used in a regulated area, does the vendor ensure continued compliance? What does it cost?

  - ***Confidentiality***. Does the agreement require the vendor to maintain the confidentiality of your data?

  - ***Remedies/Dispute Resolution***. Does the agreement permit you to withhold transaction fees as a consequence of substandard performance? Does it provide for fast track dispute resolution?

  - ***Termination***. Does the agreement provide you with flexibility to terminate without penalty?

  - ***Warranties.*** Minimum warranty of title, non-infringement and "work-person-like conduct" should be required. Does the agreement provide for

uptime and availability warranties? Performance warranties should also be considered. If detailed functional specifications, response times, transmission levels, etc. are required, you should clearly state.

- ***Maintenance Terms.*** Are severity levels defined? Are specific response times established? What are the remedies for non-performance? How long will legacy systems be serviced? Will updates require hardware updates? Maintenance fees (annual increases)?

- ***Software Escrow.*** Will source code provide value? Who pays escrow fee? How often will escrow be updated?

- ***Back-up/Disaster Recovery***. Does the agreement provide for continuity of services through catastrophic events?

- ***Deconversion Assistance***. Does the agreement require the vendor to assist in the transition to a new services vendor by providing copies of data files and other transition services?

- ***Audit/Disabling Provisions***. Does the Agreement provide for an Audit? May the vendor conduct the audit remotely? Notice should be provided. Remedies should be limited to requesting additional license fees. Software may not be disabled.

Hosting Agreements

- Some businesses contract with the developer (or another third party) to "host" the website, which means to permit the computer files containing the website to reside on the third party's computer and to receive all user traffic ("hits") to the site. In addition to the above contract issues, a Web Hosting agreement should address other areas as well.

  - ***Uptime and bandwidth guarantees***. Does the agreement set out acceptable standards of continuous availability and traffic capacity?

  - ***Security.*** Does the web host use secure server/encryption technology that assures that sensitive customer information will remain secure?

  - ***Back-up and disaster recovery capacity***. Will the host back up the site and agreed upon intervals? Does the host have a back-up server or a pan to continue your services in the event of a major server failure?

  - ***Termination/Portability***. Is the contract easily terminable and can it be moved to another host? Is the host required to cooperate by providing copies of all files so changing hosts is simplified?

  - ***Reporting.*** Does the agreement spell out what use statistics the host is required to report?

Hiring Employees/Contractors

- ***Ownership of Work Product.*** Has intellectual property created for the company been properly secured?

  - Have employees signed appropriate Confidentiality and Invention Assignment Agreement?

- Have consultants and independent contractors signed appropriate Confidentiality and Invention Assignment Agreements?

- Is a trade secret protection program appropriate?

- Have patents been applied for company-owned inventions and discoveries?

- Do development agreements define and assign ownership of source code?

- ***Non-Compete.*** Have appropriate "non-competition" clauses been included in independent contractor and employee agreements?

- Are there any employment contracts with key people that should be reviewed, or that may be coming up for renewal?

- Has the company hired any key employee who is not, but should be, a party to a written employment contract with the company?

- Are all key employees, including those with technical knowledge or expertise and those who have access to company trade secrets and confidential information, subject to adequate nondisclosure and non-competition restrictions? Are these restrictions being consistently enforced?

- Has the company established a technology/e-mail appropriate use policy?

General Intellectual Property Protection

- Trademark/servicemark registrations for company products and services?

- Is the company using the intellectual property of any third party?

  - Are all needed licenses obtained?

  - Is the company complying with all license agreements to which it is a licensee?

  - Is the company infringing the intellectual property rights of others?

- Is there a program in place to determine if others are violating the company's intellectual property rights?

- Are appropriate notices used on "published" content (trademark & copyright), as well as notice of ownership and permitted use

Regulatory Issues

- Is the business regulated by any federal or state agency?

- Have all licenses been obtained?

- Has the company limited its jurisdictional exposure?

- Does the company collect information from users?

  - Is the collection regulated? - children, legal, medical, financial, etc.

- Has the company established a privacy policy?

- Must include notice, opt-out, access & security provisions. (More may be required if information/class is regulated).

Electronic Contracting

- Is a method used to verify terms and parties to contract?
- Have appropriate "terms of sale" been included in a "click-through" agreement?
- Have appropriate disclaimers been included?

Standard SLA:	Effective SLA:
Guarantee a certain level of circuit performance over the carrier's core backbone that is consistently exceeded by its network (including availability, latency, throughput).	Guarantee a certain level of end-to-end service performance for applications.
Compensation for prolonged circuit outages is a nominal credit — usually 5% to 10% of the cost of the service.	Remedy for prolonged circuit outages is reimbursement of the cost of the back-up services used.
The protection from repeated failures is a nominal credit capped at 50% of the total monthly recurring cost.	Protection from repeated failures is the opportunity to augment/replace defective services with more reliable services from another vendor or use a different technology at no additional cost.
The options for getting out of a contract for failure over a prolonged period of time are nil.	Option for getting out of a contract for failure over a prolonged period of time is termination of the agreement without penalty, and possibly reimbursement of costs associated with integration of new technology

VII. CONTRACT MANAGEMENT

A. ***Management Process***. Upon the signing of a definitive outsourcing agreement, the most critical process has just begun. Failure to vigilantly monitor and manage an outsourced relationship is a recipe for disaster. Often, the remedies offered a Licensee under an outsourcing arrangement are only triggered upon notification from the Licensee.

B. ***Ensure that contingency plans are formulated and viable in the event of nonperformance by the service provider***. Outsourcing creates a dependency on the third-party service provider, which raises several issues that must be addressed. Concerns stem from the potential consequence of a business disruption or other problem at the service provider. In anticipation of such a situation, the financial institution needs to verify that the service provider has a prudent business recovery plan in place. The adequacy of this plan needs to be reviewed by audit as a part of the vendor selection due diligence process and on an on-going basis. More importantly, the financial institution needs to have contingency plans in the event of deteriorating performance by the service provider or other such event. Given the costs of alternative options, most financial institutions work with the third party to resolve difficulties. In the face of unsatisfactory responsiveness, an institution's options include changing service providers, returning the activity to the institution, or sometimes even exiting the business. All institutions emphasize that these are very costly options, which are often taken only as a last measure. Nevertheless, this eventuality and associated costs are increasingly being pre-specified in the contract as a part of the negotiation process. In older contracts, such clauses are added at renewal.