This material was originally published in KATHERYN A. ANDRESEN, THE LAW AND BUSINESS OF COMPUTER SOFTWARE (West Services, Inc., 2007), Ch. 12 (2d ed.)

OUTSOURCING ISSUES

By Katheryn A. Andresen and Jen C. Salyers

Although outsourcing, specifically offshore outsourcing, is currently a political hot potato, businesses have used the outsourcing concept for centuries. In the 17th century, the East India Trading Company outsourced its buyers, translators, and guides. In today's market, outsourcing allows businesses to contract for specific deliverables and services that are not a standard part of their business, but which are critical to expanding their growth.

In particular, it has become abundantly clear in the last few decades that companies in the 21st century require information technology (IT) services and access to the Internet to succeed. For many companies, these IT services may include services like network management, customer service help centers, application development/implementation/management services, data center management, and maintenance. Software service contracts, in particular, may encompass any aspect of business management: financial, human resources, distribution, or time management. A company has several options for addressing these IT service needs, including: hiring the staff needed to implement in-house; contracting with specific IT personnel for specific functions; or outsourcing the entire project and/or department for a specific deliverable or service.

Some companies have learned the hard way that deciding to keep everything in-house may cost a lot of money and be a deterrent to meeting growth goals as the company deals with IT issues that are not the primary service offered by the company. While internal staff means the company retains full control over the personnel and the security of company information, it is not necessarily the most efficient means of meeting the company's IT needs. The IT field changes daily and requires constant upgrades and modifications for advances made in both hardware and software. One government paper, which focused on financial institutions, quoted possible savings for outsourcing as:

> Deloitte Consulting, LLP estimates that financial institutions that offshore achieve average cost savings of 39 percent, with one in four institutions surveyed achieving savings of more than 50 percent. Typically, financial institutions offshore non-core job functions, such as IT (specifically, software development and maintenance), administration, human resources, contact centers, call centers, and telemarketing.[1]

Conversely, not every company has had a good experience with outsourcing. There is a limited amount of control over the quality of the service which can have a significant impact on the quality associated with the company's brand. There can be a loss or disclosure of sensitive information for which the company will still have responsibility, if not liability. The outsourcing process can actually result in losses instead of cost savings if the risks are not controlled, protected, and/or offset.

[FN1] *See* the Federal Deposit of Insurance Corporation's "Offshore Outsourcing of Data Services by Insured Institutions and Associated Consumer Privacy Risks", found at https://www.fdicconnect.gov/regulations/examinations/offshore/offshore_outsourcing_06-04-04.pdf.

§ 12:2. Complexities of outsourcing models

Outsourcing models come in dozens of variations and models. On the simplest level, an individual contractor, i.e., staff augmentation, is an outsourcing model. Outsourcing, on the other end of the complexity scale, means moving an entire department, process, or IT project to another contractor. Outsourcing, especially in the IT field, has led to a whole vocabulary and series of acronyms for the most common types of projects:

- BPO—business process outsourcing (i.e., outsourcing the Human Resources department)
- ITO—information technology outsourcing (i.e., outsourcing a specific development project and/or IT support function)
- "Staff Aug"—outsourcing as a means of staff augmentation without hiring employees directly
- Offshore—outsourcing where the contractor's entity is based outside of the continental United States. There are variations of this as well:
    - Captive Direct—company-owned subsidiary in the same country as the contractor's corporation where services are performed
    - Joint Venture—company and contractor jointly owned subsidiary provide outsourcing services
    - Third-Party Vendor Direct—vendor will use foreign subcontractors to perform services but with knowledge and consent of company
    - Third-Party Vendor Indirect—vendor uses foreign subcontractors without the knowledge or consent of company

There are also considerations as to the type of information disclosed during the outsourcing project which a company should consider in assessing the type of risk, the format of the outsourcing arrangement, and whether the outsourcing is appropriate for an offshore consideration. A graphical view of the risks associated with an offshore outsourcing arrangement is as follows:

<- Image not available ->

The information ranges from:

- low risk—nonconfidential, noncritical electronic programming code
- medium low risk—confidential, noncritical electronic files
- medium high risk—confidential, critical electronic files
- high risk—highly confidential, critical, personal/consumer information,[1] paper and electronic files

[FN1] This is typically information governed by federal regulation like the Gramm-Leach-Bliley Act or the Health Information Portability and Accountability Act; *see, generally*, §§ 6:1 et seq.

§ 12:3. Staff augmentation—"Simple outsourcing"

Staff augmentation may meet the IT needs for smaller businesses. An example might be contracting with an independent contractor to manage the company's network. This type of contracting provides a company with more flexibility to increase or decrease the number of independent contractors as the business needs change, without having the employment issues implicated when firing or terminating an employee. This type of contracting may be considered "simple outsourcing," but it is not without risks, as Microsoft discovered in the late 1990s.[1]

Like Microsoft, larger companies are often able to negotiate better service contracts due to the amount being spent on these software services. In the current market, it is common for large IT service contracts to cost millions and have initial terms anywhere from five to 10 years. At this level of cost and commitment, all companies should be willing to take the time and legal precautions necessary to ensure they receive the expected deliverables and services. This is especially critical to ensure that a company's intellectual property and company information are kept secure despite having IT contractors involved deeply in the operations of the company.

Many companies have hired independent contractors for specific projects or functions. There are both business and legal issues to be considered before contracting with an independent contractor. An independent contractor provides the expertise the company requires without paying the premium for hiring an expert as a full-time employee. The company may, however, need additional investment in facilities or systems to provide the independent contractor with the tools he or she needs to deliver the services. Since the contract is on an individual basis, the company has more control over intellectual property protections, as the independent contractor would be personally liable for violating the confidentiality clause or agreement.

Independent contractors should be hired using a written agreement. There are several questions that should be asked prior to signing a service agreement with an independent contractor: Does the contractor operate as an individual or as a corporate entity; if the contractor operates as a corporate entity, what is the structure of this entity; does the contractor have employees; is the contractor currently licensed (if licensure is a requirement for the deliverable/service); does the contractor use personalized business cards, stationery, and invoice forms; and is the contractor insured? These questions are designed in part to ensure that the independent contractor is not later deemed to be an employee for tax purposes, which developed out of the *Microsoft I* case.[2]

Heading into the start of the tech-boom in the 1990s, Microsoft found that it needed additional IT staff to meet its business needs. A decision was made to hire the additional personnel through staffing agencies on an independent-contractor basis in order to avoid the added cost of providing the benefits to which a full-time employee would be entitled. Microsoft, however, was not willing to relinquish control over the contractors and used its size and power to negotiate contracts, which were heavily weighted in Microsoft's favor, for controlling the salary, location of the work, hours, equipment, and right to terminate. Microsoft was audited by the IRS for open tax years of 1989 and 1990, and the IRS determined there were 20 factors which may be considered to determine if a “contractor” is really an employee.[3]

Microsoft failed this 20-factor test because the company treated the independent contractors like employees. These workers were ultimately deemed employees because they were: on the same teams as employees; supervised the same; performed the same functions; worked on-site; had admittance keys; and received supplies and office equipment from Microsoft. After the IRS found these workers to be employees for tax purposes, several of the independent contractors sued Microsoft to be deemed employees in order to get 401(k) plan and stock purchase plan benefits. Although Microsoft won at the district court level in the Western District of Washington, the Ninth Circuit reversed the district court and held that the independent contractors were employees.[4]

The primary test as to whether an independent contractor will be deemed an employee is whether the company has the right to control not just the end result to be accomplished, but also “the manner and means” by which the result is accomplished. The Supreme Court later reduced this 20-factor test to the 12 most-significant considerations.[5] The *Darden* factors are: skill required; source of tools and instrumentalities; location of the work; duration of the relationship of the parties; hiring party's right (or lack thereof) to assign additional projects; method of payment; hired party's role in hiring and paying assistants; whether the work is part of the hiring party's regular business; whether the hired party is in business; whether “employee benefits” are provided; and the tax treatment of the hired party.

[FN1] *See* Vizcaino v. Microsoft Corp., 97 F.3d 1187, 20 Employee Benefits Cas. (BNA) 1873, Unempl. Ins. Rep. (CCH) P 15588B, 96-2 U.S. Tax Cas. (CCH) P 50533, 78 A.F.T.R.2d 96-6690 (9th Cir. 1996), reh'g en banc granted, opinion withdrawn by, 105 F.3d 1334 (9th Cir. 1997) and on reh'g en banc, 120 F.3d 1006, 21 Employee Benefits Cas. (BNA) 1273, 97-2 U.S. Tax Cas. (CCH) P 50572, 80 A.F.T.R.2d 97-5594 (9th Cir. 1997) (“*Microsoft I*”) and §§ 11:2 to 11:3.

[FN2] *See also* §§ 11:1 et seq.

[FN3] *See* 26 C.F.R. §§ 31.3401(c)-1(b) and Rev. Rule 87-41, 1981-1 Cum Bull. 296, 2980299.

[FN4] Vizcaino v. Microsoft Corp., 97 F.3d 1187, 20 Employee Benefits Cas. (BNA) 1873, Unempl. Ins. Rep. (CCH) P 15588B, 96-2 U.S. Tax Cas. (CCH) P 50533, 78 A.F.T.R.2d 96-6690 (9th Cir. 1996), reh'g en banc granted, opinion withdrawn by, 105 F.3d 1334 (9th Cir. 1997) and on reh'g en banc, 120 F.3d 1006, 21 Employee Benefits Cas. (BNA) 1273, 97-2 U.S. Tax Cas. (CCH) P 50572, 80 A.F.T.R.2d 97-5594 (9th Cir. 1997); confirmed by Vizcaino v. Microsoft Corp., 120 F.3d 1006, 21 Employee Benefits Cas. (BNA) 1273, 97-2 U.S. Tax Cas. (CCH) P 50572, 80 A.F.T.R.2d 97-5594 (9th Cir. 1997) ("*Microsoft II*".)

[FN5] Nationwide Mut. Ins. Co. v. Darden, 503 U.S. 318, 112 S. Ct. 1344, 14 Employee Benefits Cas. (BNA) 2625 (1992); *see also* § 11:3.

§ 12:4. Outsourcing functions or projects

Generally speaking, large outsourcing contracts are less likely to fall into the *Microsoft I-II* case issues because the contracts are generally with corporate entities who maintain control over the contracted workers. As in the case of simple outsourcing, a company needs to do a cost-benefit analysis of outsourcing before entering into such a large, complex agreement. One of the first considerations is whether the function is one that requires an area of expertise not endemic to the company's business. Outsourcing a process or service which is necessary, but not part of the core operations, can save a company both time and money in the long run. The return on investment (ROI) benefits include: a reduction of risk for employment issues while still receiving quality services by expert personnel; administrative convenience; single source control of company information security through a confidentiality provision or agreement; and flexibility to contract for these services in increments according to business needs.

Additional issues may arise with large-scale outsourcing. There may be a negative impact on internal employee morale if the outsourcing leads to a reduction in workforce. In order to avoid the *Microsoft I and II* results, companies need to give up control over "the manner and means" in which the deliverables or services are provided. When entire functions are outsourced, a company must consider data security issues, as well as ensure that the outsourcing doesn't take on a life of its own through cascading work orders or scope creep. Perhaps the biggest concern, however, is what happens when the outsourcing contract concludes or fails. In addition to regaining access and control over the company information at issue, a company will need to know in advance if there will be software, hardware, or even formatting issues to be addressed to transfer that function either back in-house or to another contractor.

A Deloitte & Touche survey found that 53% of companies will ultimately attempt to renegotiate the original terms of a contract with their contractor partners, and that one-fourth of these attempts will end in the termination of the relationship.[1] Interestingly enough, longer-term contracts offer fewer cost savings to a company and may be more uncertain. These contracts do not always address changes in technology or unforeseen issues, like the Y2K issue. In addition, these longer-term contracts bind both the company and the contractor financially and functionally in a relationship that means a loss of flexibility, which is one of the key benefits to outsourcing.

[FN1] Caldwell,. "Outsourcing Backlash," InformationWeek (650 September 29, 1997, pp 14–16).

§ 12:5. Offshore outsourcing

There have been numerous United States government-funded research projects and papers written on the pros and cons of an offshore outsourcing arrangement.[1] In particular, both the costs/savings associated with offshore outsourcing, as well as the increased security risks, has been studied and reported on often over the last two decades.[2] The savings are often not as high as anticipated due to unanticipated costs with oversight requirements (e.g. paying for a company manager to conduct on-site reviews/monitoring of project work). The costs savings may also be impacted by "scope creep" and other issues which should be addressed up front between the parties starting with the request for proposal (RFP) process and continuing on through the negotiated terms of the outsourcing master agreement.

The RFP process can be used as a critical first step in the offshore outsourcing process to ensure that the contractor selected is put on notice up front as to the company's key issues. The legal section of the RFP should include, at a minimum, those key provisions that the company expects any contractor to meet. The terms of such an RFP should clearly state: (i) that the contractor must respond as to whether it accepts, accepts with modifications, or rejects such a provision; and (ii) that the RFP responses are commitments by the contractor and will be used in the final contract provisions (i.e., no more negotiation on accepted terms.)

The master outsourcing agreement is, in a large part, similar to a master services agreement for the provision of IT services (e.g. software development and/or support), but there are additional considerations:

- Local Country Agreements (Identify specific country permitted for work—based on example)
- Government Consents (Contractor's primary responsibility to acquire/maintain)
- Changes in Law (mutual cooperation to revise as necessary based on changes)
- Transition Services (details on definition and obligations—may be based on transition plan)
- Additional Safety & Security Obligations (to address cross-border issues)
- Security Relating to Competitors (based on possibility of servers used for multiple customers and restrictions thereon)
- Disaster Recovery (including in-country access)
- Modification of Tax Provision to allow for cooperation on segregation of fees and attempts to minimize legally (based on country rules)
- Audit Rights for both deliverables and country law compliance
- Additional Warranty for law compliance (both laws and government consents) as required to provide services and deliverables
- Additional Indemnification for failure to comply with government consents
- Additional Termination Right for termination due to failure to comply with government consents (allowing partial refund and/or transition costs)
- Due Diligence Rights both pre and during agreement term
- Identify Currency to be used and who bears the risk of currency fluctuations
- Export Control and Compliance requirements (both export control regulations and OFAC rules)

The format of the outsourcing agreement also is dependent on other factors, for example:

1. Which entity will host the information and systems involved?
2. Are there local country subsidiaries for both the company and the contractor involved?
3. If the company has subsidiaries or affiliated companies in the local country where the contractor will perform the services, the outsourcing agreement may require a local country addendum to cover payment, tax, language, governing law/forum, government consents, required licenses, and other terms specific to that country. A couple of benefits to such a format include: (i) the avoidance of any double taxation issues, and (ii) increased control over some of the legal and business risks associated with an offshore outsourcing arrangement.
4. What are the metrics to be used in establishing the service levels?[3]
5. The outsourcing agreement may also require a service level agreement (SLA) addendum to detail not

only the metrics used to measure service performance (i.e., 24/7 support 365 days with a 99.98% uptime), but also the process for addressing service failures, measuring performance, and modifying the performance metrics as the parties deem reasonable.

6. What type of data will be involved (e.g. noncore business, core business, customer/private, etc.)?
7. What are the specifications or standards for the hardware, software, and/or development services involved?
8. Is there third-party software required? Does the company have the right to provide the contractor with such access? Will the contractor need to purchase its own license for such third-party software?
9. What are the current company practices and/or standards regarding the function, process, or project to be outsourced?

The format of the outsourcing arrangement may be vertical, with the agreement and obligations at the parent company level, or horizontal, with the master at the United State's parent companies, but the actual services/payment obligations contracted for at the local country level. In addition, the risks and associated provisions to protect against and/or allocate such risks to one party change based on the location of the data/software and hardware. For example, if the contractor is given secure access into the company's servers to provide services, then the company still hosts the data, software and, hardware involved. If, however, the contractor hosts the data, software, and hardware involved on its own servers/system, there are additional considerations: Will the contractor maintain the data of a direct competitor to the company on its system; what are the additional firewall and other security measures necessary to protect against disclosure; and would such a competitor have access to any of the company's data, etc., during an audit of the contractors systems?

[FN1] *See, for example*, The National Academy of Public Administration's "Off-shoring: an elusive phenomenon"; found at http://www.bea.gov/papers/pdf/NAPAOff-ShoringJan06.pdf.

[FN2] *See, for example*, the Federal Deposit Insurance Corporation's updated version of "Offshore Outsourcing of Data Services by Insured Institutions and Associated Consumer Privacy Risks"; found at http://www.fdic.gov/regulations/examinations/offshore/background.html; *see also* the Federal Deposit of Insurance Corporation's "Offshore Outsourcing of Data Se rvices by Insured Institutions and Associated Consumer Privacy Risks"; found at https://www.fdicconnect.gov/regulations/examinations/offshore/offshore_outsourcing_06-04-04.pdf.

[FN3] *See* § 12:8.

§ 12:6. Specific legal protections to consider

A company should address certain legal points in either a simple or complex outsourcing deal: description of the services; payment terms (addressing fees, timing of payments, and expenses); materials/equipment; affirmative statement that relationship is as an independent contractor; warranty by the contractor that all necessary licenses and permits required are current and that liability insurance is carried; affirmation by the contractor that it is responsible for any taxes and that it is not entitled to employee benefits; definition of term and termination rights; confidentiality of company information; and dispute resolution terms.[1] The legal structure of an outsourcing deal is often completed through a master service agreement (MSA) which has basic terms for all contractual work and individual work orders (or service level agreements) for the specific definition of the project/function, the timetable for the deliverables, and the payment terms for that project.

Some of the common issues from outsourcing contracts include:
• who owns the deliverables (i.e., copyright);
• who is liable for confidentiality breaches;
• how is the intellectual property and company information protected;
• how does a company avoid having the contractor personnel deemed employees of the company;
• does the company have the right to hire any contractor personnel;

• what needs to be accomplished to ensure access to company information upon termination of the contract; and
• how much control can the company exert over the deliverables and services before running into the *Microsoft I* issues?

There are several provisions that are specific to an outsourcing MSA. These provisions specify the contractor's responsibilities and liabilities in providing contract personnel to meet the deliverables and services. A company may want the right to review résumés of the contractor's personnel and receive assurances from the contractor that these personnel are not employees of the company. In addition, the company may require a clause that these personnel are subject to a screening process for criminal backgrounds, drug testing, and/or against the "specially designated nationals" list regulated by OFAC. This type of clause may be especially critical for regulated businesses dealing in the financial, health, and insurance fields under an obligation to protect personal/consumer information.[2]

Another critical clause for IT outsourcing contracts is the "ownership" clause. When the deliverable for the contract is software or some other authored component, it is critical that the contract specify that the work will be completed on a "work for hire" basis. Under basic copyright law, the author (or programmer) of the deliverable is the copyright owner unless: (i) the author is an employee doing the work during the normal course of business for his or her employer; or (ii) the author signs a written agreement that specifies that the work will be on a "work for hire" basis. In order to avoid further complications if the copyright rights are not deemed to be appropriately classified as a "work for hire," most of these provisions continue with caveats that the contractor assigns all rights and will be contractually obligated to undertake any other action necessary to enforce the assignment of rights.

The copyright concerns in the "ownership" clause are part of the overall intellectual property and company information that should also be protected by terms in the agreement. Confidentiality clauses should be incorporated that require the contractor, as well as all of the contractor's personnel, to protect this information to maintain its confidentiality. The contractor will typically agree to return all confidential information upon the conclusion of the agreement. In addition, to fully protect the company's interests, the remedy for a breach of confidentiality needs to specifically include equitable relief (like acquiring a temporary restraining order). Confidentiality may also be addressed in a separate confidentiality or nondisclosure agreement (NDA) This type of drafting requires a clause in the master service agreement that specifically incorporates the NDA or confidentiality agreement into the main agreement. One benefit to a separate NDA is that a company may mandate that the contractor ensure all contractor personnel review and sign a copy of that agreement.

Another typical clause in an outsourcing contract is one that precludes solicitation of each other's employees. This bar on solicitation is typically limited to terms that are reasonable and likely to be upheld by a court (e.g. 12 months.) This provision, along with any non-compete provision, may have different employment law implications that should be considered based on the jurisdiction to be applied to the contract. Some states will not enforce a non-compete provision, so some of the protections intended by this provision need to be addressed separately. For example, a software contractor may be asked not to reuse code that is developed specifically for the company. The limitations on this use may be limited to a functional version of the software, or allow reuse as long as it is less than a certain percentage of the final software product. In addition, the limit on use may be specifically geared only to a certain industry or competitive market.

A company should ensure that the protections included in the master service agreement are not removed or modified in the drafting of the specific work orders. To this extent, each work order should be reviewed for possible implications to the terms of the master agreement.

[FN1] *See also* §§ 18:1 et seq., §§ 19:1 et seq., and §§ 20:1 et seq.

[FN2] *See* §§ 6:1 et seq., specifically the Gramm-Leach-Bliley Act and the Health Information Portability and Accountability Act.

§ 12:7. Conclusion

Companies should address this myriad list of issues in the outsourcing contract prior to any deliverables or services commencing. The reason for this review and inclusion of specific provisions is to avoid the *Microsoft I-II* outcomes, where contractors were deemed employees and the company was out millions of dollars in additional benefits to be paid. A well-written contract is designed to avoid conflicts during the contract and through its termination. In particular, companies should ensure that the outsourcing contract will: provide the services or deliverables needed; allow for adequate remedies if the services or deliverables are not met; avoid uncapped liability should the contract fail; allow for modifications as needed; require assurances that the personnel used do not create further liabilities (i.e.,, by requiring criminal background checks); require assurances that the contractor will indemnify the company for any third-party copyright or other violations; require assurances that the contractor and its personnel will protect the confidentiality of the company information; maintain contractual control over the quality of the deliverables or services without dictating the "manner and means" of that performance; and provide for the appropriate transfer of the deliverables or services back to in-house or to a third party should the contract fail or be terminated.

§ 12:8. [Draft] Service Level Agreement (SLA)

1. Purpose.

The purpose of this Support SLA is to formalize an arrangement between Contractor and Company to deliver specific support services, at specific levels of support, and at an agreed-upon cost. This document is intended to provide details of the provision of Services to Company. This SLA will evolve, with additional knowledge of the Company requirements, as well as the introduction of other services into the support portfolio provided to Company.

2. Scope.

The following services are provided in response to Service Tickets from Company to the Contractor in accordance with Company's case management process.

3. Services Automatically Provided.

The following services are provided in response to Service Tickets for help desk support from Company to Contractor:

3.1. Corrective maintenance :Defined as activities associated with root-cause analysis and bug-fix isolation and resolution:

3.1.1. Root-cause analysis: Analysis of the root causes of problems. Problems will be reviewed to determine their root causes, measures will be taken to correct the sources of the problems, and reports will be prepared and distributed in a timely fashion.

3.1.2. Bug fixes: Defined as the emergency repair of any system operation that does not comply with the current signed and approved system specification. This includes system errors, "hung" or halted screens, or unexpected results within the system that render it unusable for the purpose for which it was designed.

3.2. Ticket status updates—Contractor will provide direct input into Company's Service Tickets from its ___ location, or remotely from other satellite support centers within Contractor.

4. Requests for Support Specifically Covered.

4.1. Application monitoring: Every effort will be made to conduct periodic monitoring of production applications to assess application availability.

4.2. Enhancements to production application software: These will be made when an enhancement to an existing production application is required and the level of effort is less than five days. This includes changes to the application only. Should the volume and timing of enhancements impact the timely resolution of support requests, then Contractor's support manager shall inform Company's support manager and the Contractor's account manager with the intent of assigning

enhancement work to another Contractor resource.

4.3. Transition of new or modified applications: When a new or modified application is ready to be transitioned into support, planning and coordination of the necessary activities between the Contractor or Company development team and the Contractor support team will be conducted. Other requirements include:

4.3.1. Support will commence for a new or modified application 30 days after deployment.

4.3.2. The development team is expected to support the new or modified application for the first 30 days after deployment.

4.3.3. Contractor will have at their disposal the development team or previous support team to provide knowledge transfer for a period of 60 days after deployment.

4.3.4. The Support Checklist must be completed by the deployment date (30 days prior to Contractor taking ownership). Failure to do so will require continued involvement of the development team until such time as all of the required information has been provided.

4.3.5. Applications that have outstanding Service Tickets shall remain the responsibility of the development team. If this is not possible, all outstanding Service Tickets shall be identified and SLA resolution targets will not apply. In the case of outstanding severity level 1 or 2 tickets, these will be downgraded to severity 3, and Contractor will resolve these Service Tickets in a timely manner on a best effort basis.

4.3.6. Preventative maintenance—For applications considered critical (i.e.,, a criticality level of high) by Company, and when corrective maintenance activities are low, work will be conducted up to the level of effort identified, to analyze and take steps to prevent potential problems.

4.3.7. Level 2 support—Support will be provided to the extent possible by Contractor support staff in assisting Company level 2 support team members with diagnosing problems and working in partnership to their resolution, including configuration changes to Web servers.

4.3.8. Change management—Changes will be initiated for new or changed processes, practices, or policies that affect the Contractor support team and that require support team members to understand, learn, and follow.

4.3.9. Status reporting—Contractor will ensure weekly and monthly status reports are completed by Contractor support specialists and submitted to Company for each production application supported. Monthly status reports will be discussed by the Contractor support manager with Company's management to ensure that the Company is aware of the support issues and risks faced by the support team.

4.3.10. Knowledge management—Recording, storing, and retrieval of information to assist in the resolution of problems will be established and maintained. Using this approach, the need for Company to transfer problems to Contractor for level 3 application support will be reduced, thus saving money and resources, and increasing satisfaction and quality.

5. Other Services Provided.

5.1. Evaluation of new software or hardware: Evaluation or approval of new software or hardware for use within Company can be completed as needed. This includes systems developed outside of Company, such as third-party systems, or systems developed by Company.

5.2. On-call support management: Contractor's support managers are required to be on call. Compensation is based on the level of coverage outlined in Appendix A.

5.3. Level 1 and 2 support: Level 1 (help desk) and Level 2 (infrastructure support) shall be provided by Contractor for

each production application to be supported, and they shall perform their assigned duties, such as: software installation, application installation on production servers, database connections, and database changes, for the duration of this agreement.

5.4. Upgrades to application software and associated hardware: Upgrades will be performed when an upgrade to an existing system is released. This includes operating system upgrades, database upgrades, authentication software upgrades, and vendor-required upgrades.

5.5. Assistance with application usage: Advice about or education on how to use applications, including completing transactions, creating users within or for an application, or on the purpose of an application will be provided.

5.6. Assistance with application environment support: Advice about how to use, maintain, and support application environments, including application development tools, application server software, and databases will be provided.

5.7. Adaptive maintenance: Defined as activities relating to upgrades or conversions to an application due to new versions of operating environment, including operating system, application server, or database software.

5.8. Perfective maintenance: Defined as activities relating to enhancements, with effort of five days or more, to provide additional functionality to an application.

6. Services Not Provided.

6.1. Modifications to original application specification: Any functionality not specified in the current approved design specification. Changes in Company's organization or business needs (such as a reorganization or change in business practice) may make the current specification obsolete. When this occurs, Company should initiate a request for enhancement to update the system. It is highly recommended that Company manager and Contractor work closely together to anticipate future needs and prepare timely update of systems to accommodate Company's constantly changing business.

6.2. New or added interfaces to other systems.

6.3. Intranet “front ends” to existing systems.

6.4. Adding new screens or modifications to existing screens.

6.5. Report generation, if reporting tools exist for application.

6.6. Addition of data fields.

6.7. Business rules changes (such as pricing rules changes, distributor alignment, etc.).

6.8. Deployment of existing applications to new locations (defined as the issuance of more than three accounts to new location, group, or department).

6.9. Training requests.

7. Changes to Service Level Agreement.

7.1. Termination of Agreement. In the event that Company wishes to terminate this SLA agreement, a 90-day written notice of intent to terminate must be delivered by Company to Contractor.

7.2. Amendment to Agreement. Any amendment to the Terms and Conditions of this agreement would require the approval of Company and Contractor management who signed the SOW in Appendix A.

7.3 New Applications. New applications and versions implemented during the term of this agreement will move into Company's support model through Company's process. Company will be responsible for initiating and ensuring completion of the appropriate process. These applications will be incorporated into the inventory of applications supported in Appendix A of the SOW. Changes to the inventory of applications supported will be reviewed on a regular basis, and if need be, changes to the SLA will follow the process described in the Amendment to Agreement section above.

Appendix A.

1.1. Support Services: Unless otherwise specified in a SOW, Support Services consist of the following:

(a) Contractor shall promptly notify Company and/or its third party service providers ("TPSP") of any Errors in the Software or Documentation and shall resolve such Errors in accordance with the terms of this Appendix A. As part of its obligations hereunder, Contractor shall provide to Company all operational and support assistance necessary to cause Software to perform in accordance with the Acceptance Criteria and all remedial support designed to provide a Workaround or temporary Fix to an Error until the Error can be permanently corrected. Contractor shall respond to and resolve Errors pursuant to the response and resolution schedule set forth in this Appendix A. On-site Support Services shall be provided to Company at no additional cost if, in Company' reasonable judgment, such Services are necessary to resolve an Error. Except as may be approved by Company, Contractor shall not make any changes or modifications to the Software that would adversely affect Contractor's ability to provide Software Support Services or alter the functionality of the Software or materially degrade the performance of the Software, except as may be necessary on a temporary basis to maintain the continuity of the Software Support Services.

(b) Contractor shall use commercially reasonable efforts to upgrade and improve the functionality and performance of the Software. At no additional cost, Contractor shall provide to Company all Upgrades and shall provide reasonable assistance to Company to facilitate the installation and implementation of such Upgrades. Company may test all Upgrades pursuant to Article IV and shall have the option to implement any Upgrade and any failure by Company to so implement shall not affect Company's right to continue to receive Support Services except as otherwise limited in this Appendix A.

(c) Contractor shall promptly provide to Company and its Third Party Service Providers any revisions to the existing Documentation to reflect all Error Corrections and Upgrades.

(d) Contractor shall provide e-mail and toll-free telephone hotline technical support during the times set forth in the applicable SOW. If no support times are set forth in the SOW, Contractor will provide an e-mail address and toll-free telephone support number available twenty-four (24) hours per day, seven (7) days per week, year round.

(e) While on Company's premises, Contractor and Contractor's employees and agents shall abide by all Company policies and procedures, including any security and data privacy policies.

(f) If Contractor or Contractor's employees or agents are given access to any Company physical location, computing equipment, applications (e.g., email, word processing, spreadsheet, presentation, database software, etc.), or the Company computer network, Contractor and Contractor's Agents agree to use such equipment, applications, and network access in compliance with Company's policies and procedures. Contractor agrees to use such computing equipment, applications, and network access only as necessary to directly fulfill its obligations under the Agreement.

1.2. Response and Resolution SOW: Company will classify each Error reported to Contractor based on the following criteria:

Error Classification	Criteria
Severity 1	Fatal: Error that results in the loss of all Software processing capability.
Severity 2	Severe Impact: Error which disables major functions from being performed and therefore affects the normal operation of the Software during the normal working day.
Severity 3	Degraded Operations: Error disabling only certain nonessential functions and does not affect the normal operation of the Software during the normal working day.

Severity 4	Minimal Impact: Intermittent Error affecting use of certain nonessential functions of the Software.

Provided that Company provides to Contractor a detailed description of the Error along with any information reasonably requested by Contractor that may allow Contractor to verify the Error at the time Company reports the Error, Contractor shall respond to Error reports according to the following schedule:

Error Classification	Acknowledge receipt of Error report	Provide a Workaround or Fix	Provide and Error Correction or Upgrade
Severity 1	10 minutes	4 hours	8 hours
Severity 2	10 minutes	4 hours	8 hours
Severity 3	30 minutes	8 hours	5 business days
Severity 4	1 hour	5 business days	20 business days

1.3. Non-Exclusive Remedies. If Contractor is unable to meet any of its obligations in the above specified-time frames, the primary technical contacts from Contractor and Company will agree on an action plan to resolve the Error. If the primary technical contacts are unable to agree on an action plan, the matter shall be escalated to appropriate management personnel. If Contractor is unable to meet its obligations in the above-specified time frame with respect to a Severity 1 or 2 Error, then, in addition to any other remedies that Company may have under this Agreement, Company shall be entitled to receive a refund in the amount of five percent (5%) of the then current monthly Support Services fees for each occurrence of an uncured Error, which refund shall be paid to Company within thirty (30) days of such failure.

1.4. Exclusions. Contractor shall have no obligation to provide Support Services to the extent that: (a) the Software is altered, damaged or modified by any individual other than Contractor employees or agents; (b) the Error is a result of Company's negligence, abuse or misapplication of the Software; or (c) the Error results from Company's use of the Software in combination with software or hardware not authorized by Contractor. Additionally, Contractor shall only be obligated to support the then-current version of the Software and the two (2) immediately preceding versions of the Software (for purposes of this Appendix A, a version shall mean a major release of the Software typically delineated by a number to the left of the decimal point). Finally, Contractor shall have no obligation to correct any alleged Error if Company fails to incorporate any Error Correction or Upgrade that Contractor has previously provided to address such alleged Error so long as such Upgrade has been Accepted.