# Table of Contents

**How to Guide for Cloud Processing and Outsourcing** ................................................................. 4

- Overview ........................................................................................................................................... 5
- Policy Statement ................................................................................................................................ 8
- Goal ................................................................................................................................................... 8
- ISO 31000 Compliance – Risk Management.................................................................................. 9
- GDPR Data Privacy Mandate ............................................................................................................. 10
- Cloud Processing and Outsourcing Approval Standard ................................................................. 11
- Steps to implement Software as a Service (SaaS) via the Cloud ................................................... 19
- Cloud Outsource Service Provider Level Agreements and Metrics ............................................... 20
- SLA and Metrics Reporting ............................................................................................................. 25
- Finding and Selecting a Cloud Outsource Vendor ........................................................................... 27
- Outline for RFP and Negotiation of Contract Terms ....................................................................... 32

**Appendix** .................................................................................................................................. 46

- Mutual Non-Disclosure Agreement .................................................................................................. 47
- Base Case Development ..................................................................................................................... 51
- Sample Service Level Agreement ...................................................................................................... 53
- Sample Metrics for Service Level Agreements ................................................................................ 67
- Business and IT Impact Analysis Questionnaire ................................................................................ 86
- ISO - Security Process Audit Checklist ............................................................................................ 88
- Security Policy Management Objectives ........................................................................................... 88
- Corporate Security Management Objectives .................................................................................... 89
- Organizational Asset Management Objectives .................................................................................. 91
- Human Resource Security Management Objectives .......................................................................... 92
- Physical and Environmental Security Management Objectives ...................................................... 94
- Communications and Operations Management Objectives .............................................................. 95
- Information Access Control Management Objectives ...................................................................... 98
- Systems Development and Maintenance Objectives ......................................................................... 101
- Information Security Incident Management Objectives ..................................................................... 103
- DRP and Business Continuity Management Objectives ................................................................... 104
- Compliance Management Objectives ............................................................................................... 106
- Control and Security Objectives ....................................................................................................... 107

**Cloud/Outsourcing Security Checklist Looking Ahead** ................................................................... 108

**Detail Job Descriptions** ................................................................................................................ 109
- Manager of Cloud Applications ......................................................................................................... 109
- Cloud Computing Architect ............................................................................................................. 109
- Digital Brand Manager ..................................................................................................................... 109

**Cloud and Outsourcing Forms** ........................................................................................................ 110
- Outsourcing Security Compliance Agreement Form ........................................................................ 110
- Outsourcing and Cloud Security Compliance Agreement Form ..................................................... 110
- Application & File Server inventory .................................................................................................. 110

**What’s new** .................................................................................................................................... 111
How to Guide for Cloud Processing & Outsourcing

Cloud and Outsourcing Management Standard

Overview

Cloud Processing and Outsourcing do not remove the enterprise’s requirement to manage the process. A comprehensive cloud processing and/or outsourcing arrangement requires Service Level Agreement (SLA) monitoring and redefinition, as well as strategic management and other retained functions. (See cloud outsourcing approval standard under retained costs – Page 13 for a listing of frequently retained functions).

Many CIOs and business leaders are using the cloud within their enterprise data centers to take advantage of the best practices that cloud computing has established -- scalability, agility, automation, and resource sharing. Others are using third parties to accomplish the same tasks – that is outsourcing.

By using a cloud-enabled application platform, companies can choose a hybrid approach to cloud computing that employs an organization’s existing infrastructure to launch new cloud-enabled applications. This hybrid approach allows IT departments to focus on innovation for the business, reducing both capital and operational costs and automating the management of complex technologies.

Because cloud processing is related to a number of other technologies, it is best defined with:

- **Scalability**: Cloud environments allow users to access additional compute resources on-demand in response to increased application loads.
- **Shared Resources**: As a shared resource, the cloud provides flexible, automated management to distribute the computing resources among the cloud’s users.
- **Reliability and Fault-Tolerance**: Cloud environments take advantage of the built-in redundancy of the large numbers of servers that make them up by enabling high levels of availability and reliability for applications that can take advantage of this.
- **User Focused applications**: The cloud is a natural home for service-oriented applications, which need a way to easily scale as services get incorporated into other applications.
- **Computing Utility Users**: only pay for the services they use, either by subscription or transaction-based models.
- **Common Infrastructure**: By enabling IT resources to be consolidated, multiple users share a common infrastructure, allowing costs to be more effectively managed without sacrificing the security of each user’s data.
- **Service Level Agreements**: Clouds are managed dynamically based on service-level agreements that define policies like delivery parameters, costs, and other factors.
Cloud Processing and Outsourcing Approval Standard

Overview

The decision to outsource or migrate towards a cloud is complex and requires a good deal of expertise. Approval of a cloud processing and/or outsourcing agreement requires the implementation of Service Level Agreements, an initial analysis overall scope, base case analysis, vendor identification, request for price quote, vendor bid appraisal, and contract negotiation. Each of these steps must be performed successfully in order to achieve a positive decision.

Implementation of Service Level Agreements

Analysis of Cloud Outsourcing Scope

Base Case Analysis

Vendor Identification

Request for Price Quote

Vendor Selection

This is a sample of the final product and these pages are for your review and are protected by Janco’s copyright.

https://www.e-janco.com
Contract and Confidentiality Agreements

A formal contract between ENTERPRISE and the cloud provider and/or outsourcer shall exist to protect both parties. The contract shall clearly define the types of information exchanged and the purpose for so doing.

If the information being exchanged is sensitive, a binding confidentiality agreement shall be in place between ENTERPRISE and the outsourcer, whether as part of the cloud outsource contract itself or a separate non-disclosure agreement (which may be required before the main contract is negotiated).

Information shall be classified and controlled in accordance with ENTERPRISE policy.

Any information received by ENTERPRISE from the cloud outsourcer who is bound by the contract or confidentiality agreement shall be protected by appropriate classification and labeling.

Upon termination of the contract, the confidentiality arrangements shall be revisited to determine whether confidentiality has to be extended beyond the tenure of the contract.

All contracts shall be submitted to the Legal for accurate content, language and presentation.

The contract shall clearly define each party’s responsibilities toward the other by defining the parties to the contract, effective date, functions or services being provided (e.g., defined service levels), liabilities, limitations on use of subcontractors and other commercial/legal matters normal to any contract. Depending on the results of the risk assessment, various additional controls should be embedded or referenced within the contract, such as:

- Legal, regulatory and other third party obligations such as data protection/privacy laws, money laundering, etc.3;
- Information security obligations and controls such as:
  - Information security policies, procedures, standards and guidelines, normally within the context of an Information Security Management System such as that defined in ISO/IEC 27001;
  - Background checks on employees or third parties working on the contract;
  - Access controls to restrict unauthorized disclosure, modification or destruction of information, including physical and logical access controls, procedures for granting, reviewing, updating and revoking access to systems, data and facilities etc;
  - Information security incident management procedures including mandatory incident reporting;
  - Return or destruction of all information assets by the outsourcer after the completion of the outsourced activity or whenever the asset is no longer required to support the outsourced activity;
  - Copyright, patents and similar protection for any intellectual property shared with the outsourcer or developed in the course of the contract;

3 In the case of “offshore” cloud outsourcing, special consideration must be given to the ramifications of transferring information between countries or jurisdictions, particularly where privacy and similar laws may conflict. Take qualified legal advice as a matter of course.
How to Guide for Cloud Processing & Outsourcing

SLA and Metrics Reporting

The Service Level Agreement (SLA) is the central instrument for managing an outsourced function (See page 54 for sample SLA). The Manager of Cloud Applications (see page 109) with the help of the Cloud Computing Architect (see page Error! Bookmark not defined.) will track SLA (See Service Level Agreement Report Package section – page 19) fulfillment and enforce the contract terms if an SLA is not met. The Manager of Outsourcing must also take an active role in defining and redefining SLAs in order to take into account changes in the operating environment.

Prior to outsourcing it necessary to create Service Level Agreements<sup>6</sup> for the enterprise that will show the existing level of service being provided. These are created with the user in mind. Using such a set of metrics the enterprise will know how the outsource vendor is performing. The set of metrics that can be considered are listed in Figure 2.

![Figure 2 - Reporting Package](https://www.e-janco.com/)
How to Guide for Cloud Processing & Outsourcing

Identifying Potential Cloud Outsource Vendors

One individual should be made the single point of contact within the enterprise. As soon as some outsourcing vendors hear that your enterprise is in the market, they will try to corner the market and monopolize your time. Review the job description for the Manager of Cloud Applications (see page 109) to identify the characteristics of the individual who should assume that role.

To identify the list of potential cloud, outsource vendors there are a number of places that are prime sources of information. The first and foremost is to ask other professionals who have outsourced to see which vendors they evaluated; which one they selected; why vendors were eliminated and why the vendor they chose was selected.

Candidate vendors can be identified from:

- Within your enterprise at other divisions, companies or locations.
- In major metropolitan areas, like Chicago or Los Angeles, associations like the Society for Information Management (SIM) have chapters with members who would be more than willing to discuss the viable outsourcing vendors in the local area, domestic markets and the international providers.
- Trade associations in the industry of your enterprise normally have a group of IT professionals who meet to discuss common issues. In the last few years, many of these professionals have gone through the evaluation process.
- National Business associations from Ireland, European Union, India, Korea, China, Malaysia, and other nations have groups that are helping their native companies penetrate the global outsourcing market.
- The Internet can help to identify and get preliminary information on potential vendors. Caution should be used if you have no information in support of a vendor aside from a web page.

---

*We are independent of all outsourcing vendors and accept no revenue from any such enterprise. In addition, individual outsourcing vendors provide various states of quality and pricing at any one given moment. For that reason, we have not identified any specific vendor within this document.

SIM is an association that provides no outsourcing services and that is the reason we have mentioned them by name.
Criteria for Ranking Potential Cloud Outsource Vendor

Once there is a list of 20 to 30 potential vendors, it is time to start to classify them. You will have several comments on each of the potential vendors which are good, bad and indifferent. These should be recorded in some format that will insure that information is not lost. Some individuals prefer detailed file folders; others summary excel spreadsheets. Whatever works should be used:

Factors to consider are:

► Reputations of the vendor and its employees - If a vendor has a bad reputation and/or the individuals who represent the firm are not reputable that is a strong negative. In addition, several outsourcing firms pay commissions to consultants or sales agents. Are they representing the outsourcer or themselves?

► Financial strength of the vendor - A financial report like a Dun & Bradstreet should be reviewed especially if the outsourcer is a privately-held company. At some point, you will have to ask for copies of audited financial statements. In the case of some offshore companies, they will be reluctant or unable to do so. That will have to weigh into the final selection process.

► Experience of the vendor - How long have they been in the outsourcing business and your industry, and what successes and failures have they had? Do they understand your industry, and do they have any clients who are like you in size and scope?

► Client base of the vendor in cloud outsourcing - How dependent is the vendor on their largest client(s)? Does the vendor have a contract with any of your direct competitors? If they do, how do they propose a separation of your data and individuals working on your contract so that your competitive and strategic information and direction is not shared?

► Strength of the staff of the vendor - As you gather data, determine the quality and quantity of staff that the outsourcer has. If they must hire staff, in addition to any staff you may transfer to them, they may not be strong enough to support your enterprise.

► Focus of the vendor is dollars you can generate for them - If the focus is on how much business that you can provide them versus how much value they can provide to your enterprise that may be an issue.

► Insight provided by the vendor - As you communicate with the vendor do they really understand what value they can provide to you? Are they trying to sell you their own canned solution?

► Vendor can define what is a win for you - In communications with the vendor can they define what is win for your enterprise? Do they have a feel as to how long it will take to achieve a win? Will they commit to that in a contract?

► Senior management at the vendor is committed - What level of the vendor is your point of contact? Is their senior management committed to acquiring your business and supporting it? If their senior management is not committed maybe they are stretched too thin or they may be too busy.

► Vendor is committed to a big customers or new contracts - Based on the volume of new business a vendor has, they may or may not be able to support your enterprise in both the start-up phase and operations. Sales and marketing people love to brag; listen to what they say; log and follow-up as time permits.

► Vendor’s references come easily - All vendors will provide references for their successes. The challenge will be to learn about their failures and see what the vendor has done so that those failures do not occur again. Gather as much information as possible on the vendor’s business practices, honesty and commitment to its existing client base.
**Term of the Agreement**

The term of the agreement will be for a _____ year period that can be renewed _______. (Potential for an “Evergreen” arrangement whereby the outsourcing contract can be renewed automatically)  

- Renewals shall be based upon the same pricing structure (or lower if the outsourcing vendor provides a “similar” service to other at a lower rate) and terms of the current agreement, unless modified by mutual agreement.

Renewed personnel shall be identified by training and/or title within the agreement a list of roles that will be transferred to the vendor. The vendor will be responsible for all pension/healthcare/termination benefits for transferred personnel.

- The vendor will assume all risk regarding claims by affected employees for any actions which transpire after the transfer of said personnel to the vendor.
- At the enterprise’s option, the enterprise may contract certain personnel to the vendor for a defined period of time to facilitate completing a smooth transition of the functions to the vendor. The vendor will compensate the enterprise for said personnel at specified contract rates.

**Enterprise will retain the right to specify the minimum capabilities required of staff assigned by the vendor.**

- Enterprise will provide detail job descriptions for each position that the vendor will provide.
- Enterprise will retain the sole right to determine if the staff provided by the vendor meets the requirements.
- If the vendor supplies staffing that does not meet the vendor’s requirements, the vendor will be charged for all expenses incurred by Enterprise at the rate of 2 times the cost.

**Enterprise will retain the right to specify the staffing levels and positions that will be filled by the vendor.**

- Enterprise will retain the right to specify that particular positions be filled on functions outsourced.
- Enterprise will provide organizational charts and job descriptions for positions Enterprise deems as required.
- Vendor will be required to fill positions deemed as required by Enterprise with individuals who meet Enterprise’s position requirements.

---

10 Case should be taken if this approach is used. Renewal should not be automatic if SLA’s are not met and as always the fee structure should be reviewed in detail at each contract renewal.

11 Detail job descriptions should be included. A good resource for job descriptions is the “Internet and Information Technology Position Description HandiGuide” that can be found at [http://www.e-janco.com](http://www.e-janco.com)
Mutual Non-Disclosure Agreement

This Agreement is made as of the day of, 20, between , , a corporation, whose address is , (“ENTERPRISE”), and , a(n) corporation (“Cloud Outsource Bidder”).

In order to pursue the mutual business purpose ENTERPRISE and Outsource Bidder recognize that there is a need to disclose to one another certain confidential information of each party to be used only for the Business Purpose and to protect such confidential information from unauthorized use and disclosure.

In consideration of the other party's disclosure of such information, each party agrees as follows:

1. This Agreement will apply to all confidential and proprietary information disclosed by one party to the other party, including information listed in Exhibit A and other information which the disclosing party identifies in writing as confidential before or within thirty days after disclosure to the receiving party (“Confidential Information”). Each party agrees
   i.) to hold the other party’s Confidential Information in strict confidence,
   ii.) not to disclose such Confidential Information to any third parties, and
   iii.) not to use any Confidential Information for any purpose except for the Business Purpose. Each party may disclose the other party’s Confidential Information to its responsible employees with a bona fide need to know but only to the extent necessary to carry out the Business Purpose. Each party agrees to instruct all such employees not to disclose such Confidential Information to third parties, including consultants, without prior written permission of the disclosing party.

2. Confidential Information will not include information which:
   • is now, or hereafter becomes, through no act or failure to act on the part of the receiving party, generally known or available to the public;
   • was acquired by the receiving party before receiving such information from the disclosing party and without restriction as to use or disclosure,
   • is hereafter rightfully furnished to the receiving party by a third party, without restriction as to use or disclosure;
   • is information which the receiving party can document was independently developed by the receiving party; and
   • is required to be disclosed pursuant to law, providing the receiving party uses reasonable efforts to give the disclosing party reasonable notice of such required disclosure; or (vi) is disclosed with the prior written consent of the disclosing party.

3. Each party agrees not to remove any of the other party’s Confidential Information from the premises of the disclosing party without the disclosing party’s prior written approval.

This document should be reviewed by the enterprise’s legal counsel prior to its use. We are not legal counsel, we do not express any legal opinion, and we assume no responsibility for any inclusions and exclusions within this document.
Sample Metrics for Service Level Agreements

Metrics that have been used in Service Level Agreements are defined in the tables that follow. They are categorized in the following 13 areas and can be used to create specific service level agreements:

- Financial
- Staffing
- Internet – Electronic Infrastructure
- Competitive/Comparative
- Productivity
- System Development
- Reengineering – Office Automation
- Quality Assurance
- Help Desk
- Computer Operations
- Communications
- Other Technology
- Enterprise/Industry Specific
Detail Job Descriptions

Detail job descriptions are attached under separate cover for these positions

- Manager of Cloud Applications
- Cloud Computing Architect
- Digital Brand Manager
Cloud and Outsourcing Forms

Forms are attached under separate cover for these positions

- **Outsourcing Security Compliance Agreement Form**
- **Outsourcing and Cloud Security Compliance Agreement Form**
- **Application & File Server inventory**
What’s new

Version 3.6
- GDPR Mandate requirements defined
- Added Application & File Server Inventory
- Updated the included job descriptions to be compliant with all mandated requirements
- Updated all the included for to the 2019 version

Version 3.5
- Added Cloud/Outsourcing Security Checklist Looking Ahead
- Job description included as separate documents
- Forms include as separate documents
- Updated all job descriptions to meet the latest compliance mandates
- Updated all the electronic forms to meet the latest compliance mandates
- Added Outsourcing and Outsourcing Compliance Agreement

Version 3.4
- Steps to implement Software as a Service (SaaS) via the cloud
- Updated all job descriptions
- Added Digital Brand Manager Job Description
- Re-formatted the entire document to make it easier to read and to be published for an eReader application

Version 3.3
- Updated to include BYOD and social networking issues
- Updated Business and IT Impact Questionnaire – included as a separate document
- Added the updated Business and IT Impact Questionnaire

Version 3.2
- Updated to meet all ISO, mandated, and industry security and business continuity requirements. Includes section on new ISO 31000 Risk Management Standard
- Updated Business and IT Impact Questionnaire
- Updated to meet ISO compliance requirements
- Updated for mobile devices (including BYOD)
- Updated to meet mandated cloud security requirements
- Updated non-enterprise users’ section
- Updated for to an electronic form Outsourcing Security Compliance Agreement
How to Guide for Cloud Processing & Outsourcing

Version 3.1
- Updated Risk Assessment – Business and IT Impact Questionnaire
- Updated for COBIT compliance
- Updated for PCI-DSS compliance
- Updated for US state level compliance (New York, Massachusetts, and California)
- Update for ISO security requirements
- Updated Outsourcing Policy
- Added Outsource Security Policy Compliance Agreement

Version 3.0
- Updated to use WORD CSS style sheet
- Update Business and IT Impact Questionnaire – in addition to being included as part of the main document it is included as a separate PDF and Word document.

Version 2.2
- Updated text to conform to Sarbanes-Oxley
- Updated contract terms to include staffing approval requirements
- Added section of criteria for selecting vendor candidates
- Updated ISO Security Audit Checklist to meet ISO 27001 and ISO 27002
- Updated graphics

Version 2.1
- Updated text to conform to Sarbanes-Oxley
- Added updated Business and IT Impact Questionnaire
- Added ISO 17799 Security Audit Checklist
- Added Outsource Security Policy Compliance Agreement
- Added HIPAA Audit Program Guide
- Updated selected graphics
- Corrected minor errata

Version 1.1
- Added section on cloud outsourcing metrics and service level agreements
- Add metrics best practices
- Updates Security Process Audit Checklist with finalized ISO 27031 requirements

Version 1.0
- First Published