CONTRACT BETWEEN THE CITY OF AUSTIN ("City")
AND
CREATIVE ENTERPRISE SOLUTIONS, LLC ("Contractor")
for
Information Technology Service Management Software Solution
Contract - MA 8100 NA190000118

The City accepts the Contractor's Offer (as referenced in Section 1.1.3 below) for the above requirement and enters into the following Contract.

This Contract is between Creative Enterprise Solutions, LLC having offices at 60 E Rio Salado Pkwy Suite 900, Tempe, AZ 85281 and the City, a home-rule municipality incorporated by the State of Texas, and is effective as of the date executed by the City ("Effective Date").

Capitalized terms used but not defined herein have the meanings given them in Solicitation Number RFP 8100 PAX3147.

1.1 **This Contract is composed of the following documents:**

1.1.1 This Contract

1.1.2 The City's Solicitation, Request for Proposal (RFP), 8100 PAX3147 including all documents incorporated by reference

1.1.3 Creative Enterprise Solutions, LLC Offer, dated 01/14/2019, including subsequent clarifications

1.1.4 Cherwell Software's Cherwell End-user Subscription Agreement

1.2 **Order of Precedence.** Any inconsistency or conflict in the Contract documents shall be resolved by giving precedence in the following order:

1.2.1 This Contract

1.2.2 The City's Solicitation as referenced in Section 1.1.2, including all documents incorporated by reference

1.2.3 The Contractor's Offer as referenced in Section 1.1.3, including subsequent clarifications.

1.2.4 Cherwell Software's Cherwell End-user Subscription Agreement and Hosting Services Addendum

1.1 **Term of Contract.**

1.1.1 **Term of Contract**. The Contract shall commence upon execution, unless otherwise specified, and shall remain in effect for an initial term of 36 months. The license term (including maintenance and support) shall begin upon contract execution . The Contract may be extended beyond the initial term for up to two additional 12 month periods at the City's sole option.

1.1.1.1 If the City exercises any extension option, all terms, conditions, and provisions of the Contract shall remain in effect for that extension period, subject only to any economic price adjustment otherwise allowed under the Contract.

1.1.1.2 Upon expiration of the initial term or any period of extension, the Contractor agrees to hold over under the terms and conditions of this Contract for such a period of time as is

reasonably necessary for the City to re-solicit and/or complete the deliverables due under the Contract (not to exceed 120 calendar days unless mutually agreed to in writing).

1.2 **Compensation.** The Contractor shall be paid a total Not-to-Exceed amount of $$334,825.00 for the initial Contract term, $55,650.00 for the first extension option, and $58,512.00 for the second extension options for the total contract amount of $448,987.00. Reasonable and actual travel expenses for on-site work, not to exceed the following estimates, will be billed in accordance with GSA's guidelines.

No.	Software Licensing and Implementation Services	Unit	Extended Price
1	Base Software Licensing Cost (Service Request Fulfillment, Change Management, Problem Management, and Incident Management)	25 Units / $1,800	$45,000.00
2	Additional software licensing costs (if applicable) - Customer Self Service Portal (included in Line 1)		
3	Implementation: Software Services		$67,650.00
4	Implementation: Project Management		$12,375.00
5	Implementation: Additional Personnel Resources (interfaces, integration, customizations to support ABIA staff): Design		$15,600.00
6	Training for up to 10 staff (on site)	10	$14,500.00
7	Additional Training Resources/Options (web based, off-site, other modes) – 8 hours of remote-training	20	$1,650.00
8	Professional Service	NTE	$60,000.00
9	Not to Exceed Travel Expenses Amount (for Line 5 and Line 6)	1	$4,200.00
	Total Price of Software and Implementation Services		**$220,975.00**

	Year 1 - Maintenance and Support	Units	Extended Price
10	Licenses and Software Maintenance and Support (included in Line 1)	12 Months	
11	On-Site Professional Services (2.5-days consecutive on-site)	20 hours	$4,950.00
12	Not to Exceed Travel Expenses Amount (for Line 12)		$1,350.00
13	Training for up to 5 staff (8 hours of remote training)	5	$1,650.00
	Total		**$7,950.00**

Item No.	Year 2 - Maintenance and Support	Unit	Extended Price
15	Subscription Licenses, Software Maintenance and Support	12 Months	$45,000.00
16	On-Site Professional Services (2.5-days consecutive on-site)	20 hours	$4,950.00

Item No.		Unit	Extended Price
17	Not to Exceed Travel Expenses Amount (for Line 16)		$1,350.00
18	Training for up to 5 staff (8 hours of remote training)	5	$1,650.00
	Total		**$52,950.00**

Item No.	Year 3 - Maintenance and Support	Unit	Extended Price
19	Subscription Licenses, Software Maintenance and Support	12 Months	$45,000.00
20	On-Site Professional Services (2.5-days consecutive on-site)	20 hours	$4,950.00
21	Not to Exceed Travel Expenses Amount (for Line 20)		$1,350.00
22	Training for up to 5 staff (8 hours of remote training)	5	$1,650.00
	Total		**$52,950.00**

	3 Years/36 Months Total		$334,825.00

Item No.	Extension Option 1 - Maintenance and Support	Unit	Extended Price
23	Subscription Licenses, Software Maintenance and Support	12 Months	$47,700.00
24	On-Site Professional Services (2.5-days consecutive on-site)	20 hours	$4,950.00
25	Not to Exceed Travel Expenses Amount (for Line 25)		$1,350.00
26	Training for up to 5 staff (8 hours of remote training)	5	$1,650.00
	Total		**$55,650.00**

Item No.	Extension Option 2 -Maintenance and Support	Unit	Extended Price
27	Subscription Licenses, Software Maintenance and Support	12 Months	$50,562.00
28	On-Site Professional Services (2.5-days consecutive on-site)	20 hours	$4,950.00
29	Not to Exceed Travel Expenses Amount (for Line 28)		$1,350.00
30	Training for up to 5 staff (8 hours of remote training)	5	$1,650.00
	Total		**$58,512.00**

	Extension Options Total		$114,162.00

	Total Contract Not to Exceed		$448,987.00

1.3 **Quantity of Work.** There is no guaranteed quantity of work for the period of the Contract and there are no minimum order quantities. Work will be on an as needed basis as specified by the City for each Delivery Order

This Contract (including any Exhibits) constitutes the entire agreement of the parties regarding the subject matter of this Contract and supersedes all prior and contemporaneous agreements and understandings, whether written or oral, relating to such subject matter. This Contract may be altered, amended, or modified only by a written instrument signed by the duly authorized representatives of both parties.

In witness whereof, the parties have caused a duly authorized representative to execute this Contract on the date set forth below.

CREATIVE ENTERPRISE SOLUTIONS, LLC	CITY OF AUSTIN
Brian Flora	Sai Xoomsai Purcell
Printed Name of Authorized Person	Printed Name of Authorized Person
Signature	Signature
Principal	Procurement Supervisor
Title:	Title:
08/05/2019	8 8 19
Date:	Date:

CITY OF AUSTIN
PURCHASING OFFICE
STANDARD PURCHASE TERMS AND CONDITIONS

By submitting an Offer in response to the Solicitation, the Contractor agrees that the Contract shall be governed by the following terms and conditions. Unless otherwise specified in the Contract, Sections 3, 4, 5, 6, 7, 8, 20, 21, and 36 shall apply only to a Solicitation to purchase Goods, and Sections 9, 10, 11 and 22 shall apply only to a Solicitation to purchase Services to be performed principally at the City's premises or on public rights-of-way.

1. **CONTRACTOR'S OBLIGATIONS**. The Contractor shall fully and timely provide all Deliverables described in the Solicitation and in the Contractor's Offer in strict accordance with the terms, covenants, and conditions of the Contract and all applicable Federal, State, and local laws, rules, and regulations.

2. **EFFECTIVE DATE/TERM**. Unless otherwise specified in the Solicitation, this Contract shall be effective as of the date the contract is signed by the City, and shall continue in effect until all obligations are performed in accordance with the Contract.

3. **CONTRACTOR TO PACKAGE DELIVERABLES**: The Contractor will package Deliverables in accordance with good commercial practice and shall include a packing list showing the description of each item, the quantity and unit price Unless otherwise provided in the Specifications or Supplemental Terms and Conditions, each shipping container shall be clearly and permanently marked as follows: (a) The Contractor's name and address, (b) the City's name, address and purchase order or purchase release number and the price agreement number if applicable, (c) Container number and total number of containers, e.g. box 1 of 4 boxes, and (d) the number of the container bearing the packing list. The Contractor shall bear cost of packaging. Deliverables shall be suitably packed to secure lowest transportation costs and to conform with requirements of common carriers and any applicable specifications. The City's count or weight shall be final and conclusive on shipments not accompanied by packing lists.

4. **SHIPMENT UNDER RESERVATION PROHIBITED**: The Contractor is not authorized to ship the Deliverables under reservation and no tender of a bill of lading will operate as a tender of Deliverables.

5. **TITLE & RISK OF LOSS**: Title to and risk of loss of the Deliverables shall pass to the City only when the City actually receives and accepts the Deliverables.

6. **DELIVERY TERMS AND TRANSPORTATION CHARGES**: Deliverables shall be shipped F.O.B. point of delivery unless otherwise specified in the Supplemental Terms and Conditions. Unless otherwise stated in the Offer, the Contractor's price shall be deemed to include all delivery and transportation charges. The City shall have the right to designate what method of transportation shall be used to ship the Deliverables. The place of delivery shall be that set forth in the block of the purchase order or purchase release entitled "Receiving Agency".

7. **RIGHT OF INSPECTION AND REJECTION**: The City expressly reserves all rights under law, including, but not limited to the Uniform Commercial Code, to inspect the Deliverables at delivery before accepting them, and to reject defective or non-conforming Deliverables. If the City has the right to inspect the Contractor's, or the Contractor's Subcontractor's, facilities, or the Deliverables at the Contractor's, or the Contractor's Subcontractor's, premises, the Contractor shall furnish, or cause to be furnished, without additional charge, all reasonable facilities and assistance to the City to facilitate such inspection.

8. **NO REPLACEMENT OF DEFECTIVE TENDER**: Every tender or delivery of Deliverables must fully comply with all provisions of the Contract as to time of delivery, quality, and quantity. Any non-complying tender shall constitute a breach and the Contractor shall not have the right to substitute a conforming tender; provided, where the time for performance has not yet expired, the Contractor may notify the City of the intention to cure and may then make a conforming tender within the time allotted in the contract.

9. **PLACE AND CONDITION OF WORK**: The City shall provide the Contractor access to the sites where the Contractor is to perform the services as required in order for the Contractor to perform the services in a timely and efficient manner, in accordance with and subject to the applicable security laws, rules, and regulations. The Contractor acknowledges that it has satisfied itself as to the nature of the City's service requirements and specifications, the location and essential characteristics of the work sites, the quality and quantity of materials, equipment, labor and facilities necessary to perform the services, and any other condition or state of fact which could in any way affect performance of the Contractor's obligations under the contract. The Contractor hereby releases and holds the City

harmless from and against any liability or claim for damages of any kind or nature if the actual site or service conditions differ from expected conditions.

10. **WORKFORCE**

   A.   The Contractor shall employ only orderly and competent workers, skilled in the performance of the services which they will perform under the Contract.

   B.   The Contractor, its employees, subcontractors, and subcontractor's employees may not while engaged in participating or responding to a solicitation or while in the course and scope of delivering goods or services under a City of Austin contract or on the City's property .

        i.   use or possess a firearm, including a concealed handgun that is licensed under state law, except as required by the terms of the contract; or
        ii.   use or possess alcoholic or other intoxicating beverages, illegal drugs or controlled substances, nor may such workers be intoxicated, or under the influence of alcohol or drugs, on the job.

   C.   If the City or the City's representative notifies the Contractor that any worker is incompetent, disorderly or disobedient, has knowingly or repeatedly violated safety regulations, has possessed any firearms, or has possessed or was under the influence of alcohol or drugs on the job, the Contractor shall immediately remove such worker from Contract services, and may not employ such worker again on Contract services without the City's prior written consent.

11. **COMPLIANCE WITH HEALTH, SAFETY, AND ENVIRONMENTAL REGULATIONS**: The Contractor, its Subcontractors, and their respective employees, shall comply fully with all applicable federal, state, and local health, safety, and environmental laws, ordinances, rules and regulations in the performance of the services, including but not limited to those promulgated by the City and by the Occupational Safety and Health Administration (OSHA). In case of conflict, the most stringent safety requirement shall govern. The Contractor shall indemnify and hold the City harmless from and against all claims, demands, suits, actions, judgments, fines, penalties and liability of every kind arising from the breach of the Contractor's obligations under this paragraph.

12. **INVOICES**:

   A.   The Contractor shall submit separate invoices in duplicate on each purchase order or purchase release after each delivery. If partial shipments or deliveries are authorized by the City, a separate invoice must be sent for each shipment or delivery made.

   B.   **Proper Invoices must include a unique invoice number, the purchase order or delivery order number and the master agreement number if applicable, the Department's Name, and the name of the point of contact for the Department**. Invoices shall be itemized and transportation charges, if any, shall be listed separately. A copy of the bill of lading and the freight waybill, when applicable, shall be attached to the invoice. The Contractor's name and, if applicable, the tax identification number on the invoice must exactly match the information in the Vendor's registration with the City. Unless otherwise instructed in writing, the City may rely on the remittance address specified on the Contractor's invoice.

   C.   Invoices for labor shall include a copy of all time-sheets with trade labor rate and Deliverables order number clearly identified. Invoices shall also include a tabulation of work-hours at the appropriate rates and grouped by work order number. Time billed for labor shall be limited to hours actually worked at the work site.

   D.   Unless otherwise expressly authorized in the Contract, the Contractor shall pass through all Subcontract and other authorized expenses at actual cost without markup.

   E.   Federal excise taxes, State taxes, or City sales taxes must not be included in the invoiced amount. The City will furnish a tax exemption certificate upon request.

CITY OF AUSTIN
PURCHASING OFFICE
STANDARD PURCHASE TERMS AND CONDITIONS

13. **PAYMENT**:

A. All proper invoices received by the City will be paid within thirty (30) calendar days of the City's receipt of the Deliverables or of the invoice, whichever is later.

B. **If payment is not timely made, (per paragraph A), interest shall accrue on the unpaid balance at the lesser of the rate specified in Texas Government Code Section 2251.025 or the maximum lawful rate; except, if payment is not timely made for a reason for which the City may withhold payment hereunder, interest shall not accrue until ten (10) calendar days after the grounds for withholding payment have been resolved.**

C. If partial shipments or deliveries are authorized by the City, the Contractor will be paid for the partial shipment or delivery, as stated above, provided that the invoice matches the shipment or delivery.

D. The City may withhold or set off the entire payment or part of any payment otherwise due the Contractor to such extent as may be necessary on account of:

   i. delivery of defective or non-conforming Deliverables by the Contractor;
   ii. third party claims, which are not covered by the insurance which the Contractor is required to provide, are filed or reasonable evidence indicating probable filing of such claims;
   iii. failure of the Contractor to pay Subcontractors, or for labor, materials or equipment;
   iv. damage to the property of the City or the City's agents, employees or contractors, which is not covered by insurance required to be provided by the Contractor;
   v. reasonable evidence that the Contractor's obligations will not be completed within the time specified in the Contract, and that the unpaid balance would not be adequate to cover actual or liquidated damages for the anticipated delay;
   vi. failure of the Contractor to submit proper invoices with all required attachments and supporting documentation; or
   vii. failure of the Contractor to comply with any material provision of the Contract Documents.

E. Notice is hereby given of Article VIII, Section 1 of the Austin City Charter which prohibits the payment of any money to any person, firm or corporation who is in arrears to the City for taxes, and of §2-8-3 of the Austin City Code concerning the right of the City to offset indebtedness owed the City.

F. Payment will be made by check unless the parties mutually agree to payment by credit card or electronic transfer of funds. The Contractor agrees that there shall be no additional charges, surcharges, or penalties to the City for payments made by credit card or electronic funds transfer.

G. The awarding or continuation of this contract is dependent upon the availability of funding. The City's payment obligations are payable only and solely from funds Appropriated and available for this contract. The absence of Appropriated or other lawfully available funds shall render the Contract null and void to the extent funds are not Appropriated or available and any Deliverables delivered but unpaid shall be returned to the Contractor. The City shall provide the Contractor written notice of the failure of the City to make an adequate Appropriation for any fiscal year to pay the amounts due under the Contract, or the reduction of any Appropriation to an amount insufficient to permit the City to pay its obligations under the Contract. In the event of non or inadequate appropriation of funds, there will be no penalty nor removal fees charged to the City.

14. **TRAVEL EXPENSES**: All travel, lodging and per diem expenses in connection with the Contract for which reimbursement may be claimed by the Contractor under the terms of the Solicitation will be reviewed against the City's Travel Policy as published and maintained by the City's Controller's Office and the Current United States General Services Administration Domestic Per Diem Rates (the "Rates") as published and maintained on the Internet at:

http://www.gsa.gov/portal/category/21287

No amounts in excess of the Travel Policy or Rates shall be paid. All invoices must be accompanied by copies of detailed itemized receipts (e.g. hotel bills, airline tickets). No reimbursement will be made for expenses not actually incurred. Airline fares in excess of coach or economy will not be reimbursed. Mileage charges may not exceed the amount permitted as a deduction in any year under the Internal Revenue Code or Regulations.

15. **FINAL PAYMENT AND CLOSE-OUT**:

   A. If an MBE/WBE Program Compliance Plan is required by the Solicitation, and the Contractor has identified Subcontractors, the Contractor is required to submit a Contract Close-Out MBE/WBE Compliance Report to the Project manager or Contract manager no later than the 15th calendar day after completion of all work under the contract. Final payment, retainage, or both may be withheld if the Contractor is not in compliance with the requirements of the Compliance Plan as accepted by the City.

   B. The making and acceptance of final payment will constitute:

      i. a waiver of all claims by the City against the Contractor, except claims (1) which have been previously asserted in writing and not yet settled, (2) arising from defective work appearing after final inspection, (3) arising from failure of the Contractor to comply with the Contract or the terms of any warranty specified herein, (4) arising from the Contractor's continuing obligations under the Contract, including but not limited to indemnity and warranty obligations, or (5) arising under the City's right to audit; and

      ii. a waiver of all claims by the Contractor against the City other than those previously asserted in writing and not yet settled.

16. **SPECIAL TOOLS & TEST EQUIPMENT**: If the price stated on the Offer includes the cost of any special tooling or special test equipment fabricated or required by the Contractor for the purpose of filling this order, such special tooling equipment and any process sheets related thereto shall become the property of the City and shall be identified by the Contractor as such.

17. **AUDITS and RECORDS**:

   A. The Contractor agrees that the representatives of the Office of the City Auditor or other authorized representatives of the City shall have access to, and the right to audit, examine, or reproduce, any and all records of the Contractor related to the performance under this Contract. The Contractor shall retain all such records for a period of three (3) years after final payment on this Contract or until all audit and litigation matters that the City has brought to the attention of the Contractor are resolved, whichever is longer. The Contractor agrees to refund to the City any overpayments disclosed by any such audit.

   B. Records Retention:

      i. Contractor is subject to City Code chapter 2-11 (Records Management), and as it may subsequently be amended. For purposes of this subsection, a Record means all books, accounts, reports, files, and other data recorded or created by a Contractor in fulfillment of the Contract whether in digital or physical format, except a record specifically relating to the Contractor's internal administration.

      ii. All Records are the property of the City. The Contractor may not dispose of or destroy a Record without City authorization and shall deliver the Records, in all requested formats and media, along with all finding aids and metadata, to the City at no cost when requested by the City

      iii. The Contractor shall retain all Records for a period of three (3) years after final payment on this Contract or until all audit and litigation matters that the City has brought to the attention of the Contractor are resolved, whichever is longer.

   C. The Contractor shall include sections A and B above in all subcontractor agreements entered into in connection with this Contract.

18. **SUBCONTRACTORS**:

A. If the Contractor identified Subcontractors in an MBE/WBE Program Compliance Plan or a No Goals Utilization Plan the Contractor shall comply with the provisions of Chapters 2-9A, 2-9B, 2-9C, and 2-9D, as applicable, of the Austin City Code and the terms of the Compliance Plan or Utilization Plan as approved by the City (the "Plan"). The Contractor shall not initially employ any Subcontractor except as provided in the Contractor's Plan. The Contractor shall not substitute any Subcontractor identified in the Plan, unless the substitute has been accepted by the City in writing in accordance with the provisions of Chapters 2-9A, 2-9B, 2-9C and 2-9D, as applicable. No acceptance by the City of any Subcontractor shall constitute a waiver of any rights or remedies of the City with respect to defective Deliverables provided by a Subcontractor. If a Plan has been approved, the Contractor is additionally required to submit a monthly Subcontract Awards and Expenditures Report to the Contract Manager and the Purchasing Office Contract Compliance Manager no later than the tenth calendar day of each month.

B. Work performed for the Contractor by a Subcontractor shall be pursuant to a written contract between the Contractor and Subcontractor. The terms of the subcontract may not conflict with the terms of the Contract, and shall contain provisions that:

   i. require that all Deliverables to be provided by the Subcontractor be provided in strict accordance with the provisions, specifications and terms of the Contract;
   ii. prohibit the Subcontractor from further subcontracting any portion of the Contract without the prior written consent of the City and the Contractor. The City may require, as a condition to such further subcontracting, that the Subcontractor post a payment bond in form, substance and amount acceptable to the City;
   iii. require Subcontractors to submit all invoices and applications for payments, including any claims for additional payments, damages or otherwise, to the Contractor in sufficient time to enable the Contractor to include same with its invoice or application for payment to the City in accordance with the terms of the Contract;
   iv. require that all Subcontractors obtain and maintain, throughout the term of their contract, insurance in the type and amounts specified for the Contractor, with the City being a named insured as its interest shall appear; and
   v. require that the Subcontractor indemnify and hold the City harmless to the same extent as the Contractor is required to indemnify the City.

C. The Contractor shall be fully responsible to the City for all acts and omissions of the Subcontractors just as the Contractor is responsible for the Contractor's own acts and omissions. Nothing in the Contract shall create for the benefit of any such Subcontractor any contractual relationship between the City and any such Subcontractor, nor shall it create any obligation on the part of the City to pay or to see to the payment of any moneys due any such Subcontractor except as may otherwise be required by law.

D. The Contractor shall pay each Subcontractor its appropriate share of payments made to the Contractor not later than ten (10) calendar days after receipt of payment from the City.

19. **WARRANTY-PRICE**:

A. The Contractor warrants the prices quoted in the Offer are no higher than the Contractor's current prices on orders by others for like Deliverables under similar terms of purchase.

B. The Contractor certifies that the prices in the Offer have been arrived at independently without consultation, communication, or agreement for the purpose of restricting competition, as to any matter relating to such fees with any other firm or with any competitor.

C. In addition to any other remedy available, the City may deduct from any amounts owed to the Contractor, or otherwise recover, any amounts paid for items in excess of the Contractor's current prices on orders by others for like Deliverables under similar terms of purchase.

20. **WARRANTY – TITLE**: The Contractor warrants that it has good and indefeasible title to all Deliverables furnished under the Contract, and that the Deliverables are free and clear of all liens, claims, security interests and encumbrances. The Contractor shall indemnify and hold the City harmless from and against all adverse title claims to the Deliverables.

21. **WARRANTY – DELIVERABLES**: Cherwell End-user Subscription Agreement and Cherwell Hosting Services addendum.

22. **WARRANTY – SERVICES**: The Contractor warrants and represents that all services to be provided the City under the Contract will be fully and timely performed in a good and workmanlike manner in accordance with generally accepted industry standards and practices, the terms, conditions, and covenants of the Contract, and all applicable Federal, State and local laws, rules or regulations.

    A. The Contractor may not limit, exclude or disclaim the foregoing warranty or any warranty implied by law, and any attempt to do so shall be without force or effect.

    B. Unless otherwise specified in the Contract, the warranty period shall be at least one year from the Acceptance Date. If during the warranty period, one or more of the above warranties are breached, the Contractor shall promptly upon receipt of demand perform the services again in accordance with above standard at no additional cost to the City. All costs incidental to such additional performance shall be borne by the Contractor. The City shall endeavor to give the Contractor written notice of the breach of warranty within thirty (30) calendar days of discovery of the breach warranty, but failure to give timely notice shall not impair the City's rights under this section.

    C. If the Contractor is unable or unwilling to perform its services in accordance with the above standard as required by the City, then in addition to any other available remedy, the City may reduce the amount of services it may be required to purchase under the Contract from the Contractor, and purchase conforming services from other sources. In such event, the Contractor shall pay to the City upon demand the increased cost, if any, incurred by the City to procure such services from another source.

23. **ACCEPTANCE OF INCOMPLETE OR NON-CONFORMING DELIVERABLES**: If, instead of requiring immediate correction or removal and replacement of defective or non-conforming Deliverables, the City prefers to accept it, the City may do so. The Contractor shall pay all claims, costs, losses and damages attributable to the City's evaluation of and determination to accept such defective or non-conforming Deliverables. If any such acceptance occurs prior to final payment, the City may deduct such amounts as are necessary to compensate the City for the diminished value of the defective or non-conforming Deliverables. If the acceptance occurs after final payment, such amount will be refunded to the City by the Contractor.

24. **RIGHT TO ASSURANCE**: Whenever one party to the Contract in good faith has reason to question the other party's intent to perform, demand may be made to the other party for written assurance of the intent to perform. In the event that no assurance is given within the time specified after demand is made, the demanding party may treat this failure as an anticipatory repudiation of the Contract.

25. **STOP WORK NOTICE**: The City may issue an immediate Stop Work Notice in the event the Contractor is observed performing in a manner that is in violation of Federal, State, or local guidelines, or in a manner that is determined by the City to be unsafe to either life or property. Upon notification, the Contractor will cease all work until notified by the City that the violation or unsafe condition has been corrected. The Contractor shall be liable for all costs incurred by the City as a result of the issuance of such Stop Work Notice.

26. **DEFAULT**: The Contractor shall be in default under the Contract if the Contractor (a) fails to fully, timely and faithfully perform any of its material obligations under the Contract, (b) fails to provide adequate assurance of performance under Paragraph 24, (c) becomes insolvent or seeks relief under the bankruptcy laws of the United States or (d) makes a material misrepresentation in Contractor's Offer, or in any report or deliverable required to be submitted by the Contractor to the City.

27. **TERMINATION FOR CAUSE:**. In the event of a default by the Contractor, the City shall have the right to terminate the Contract for cause, by written notice effective ten (10) calendar days, unless otherwise specified, after the date of such notice, unless the Contractor, within such ten (10) day period, cures such default, or provides evidence sufficient to prove to the City's reasonable satisfaction that such default does not, in fact, exist. The City may place Contractor on probation for a specified period of time within which the Contractor must correct any non-compliance issues. Probation shall not normally be for a period of more than nine (9) months, however, it may be for a longer period, not to exceed one (1) year depending on the circumstances. If the City determines the Contractor has failed to perform satisfactorily during the probation period, the City may proceed with suspension. In the event of a default by the Contractor, the City may suspend or debar the Contractor in accordance with the "City of Austin Purchasing Office Probation, Suspension and Debarment Rules for Vendors" and remove the Contractor from the City's vendor list for up to five (5) years and any Offer submitted by the Contractor may be disqualified for up to five (5) years. In addition to any other remedy available under law or in equity, the City shall be entitled to recover all actual damages, costs, losses and expenses, incurred by the City as a result of the Contractor's default, including, without limitation, cost of cover, reasonable attorneys' fees, court costs, and prejudgment and post-judgment interest at the maximum lawful rate. All rights and remedies under the Contract are cumulative and are not exclusive of any other right or remedy provided by law.

28. **TERMINATION WITHOUT CAUSE**: The City shall have the right to terminate the Contract, in whole or in part, without cause any time upon thirty (30) calendar days' prior written notice. Upon receipt of a notice of termination, the Contractor shall promptly cease all further work pursuant to the Contract, with such exceptions, if any, specified in the notice of termination. The City shall pay the Contractor, to the extent of funds Appropriated or otherwise legally available for such purposes, for all goods delivered and services performed and obligations incurred prior to the date of termination in accordance with the terms hereof.

29. **FRAUD**: Fraudulent statements by the Contractor on any Offer or in any report or deliverable required to be submitted by the Contractor to the City shall be grounds for the termination of the Contract for cause by the City and may result in legal action.

30. **DELAYS**:

    A.   The City may delay scheduled delivery or other due dates by written notice to the Contractor if the City deems it is in its best interest. If such delay causes an increase in the cost of the work under the Contract, the City and the Contractor shall negotiate an equitable adjustment for costs incurred by the Contractor in the Contract price and execute an amendment to the Contract. The Contractor must assert its right to an adjustment within thirty (30) calendar days from the date of receipt of the notice of delay. Failure to agree on any adjusted price shall be handled under the Dispute Resolution process specified in paragraph 48. However, nothing in this provision shall excuse the Contractor from delaying the delivery as notified.

    B.   Neither party shall be liable for any default or delay in the performance of its obligations under this Contract if, while and to the extent such default or delay is caused by acts of God, fire, riots, civil commotion, labor disruptions, sabotage, sovereign conduct, or any other cause beyond the reasonable control of such Party. In the event of default or delay in contract performance due to any of the foregoing causes, then the time for completion of the services will be extended; provided, however, in such an event, a conference will be held within three (3) business days to establish a mutually agreeable period of time reasonably necessary to overcome the effect of such failure to perform.

31. **INDEMNITY**:

    A.   Definitions:

        i.   "Indemnified Claims" shall include any and all claims, demands, suits, causes of action, judgments and liability of every character, type or description, including all reasonable costs and expenses of litigation, mediation or other alternate dispute resolution mechanism, including attorney and other professional fees for:

      (1)   damage to or loss of the property of any person (including, but not limited to the City, the Contractor, their respective agents, officers, employees and subcontractors; the officers, agents, and employees of such subcontractors; and third parties); and/or

      (2)   death, bodily injury, illness, disease, worker's compensation, loss of services, or loss of income or wages to any person (including but not limited to the agents, officers and employees of the City, the Contractor, the Contractor's subcontractors, and third parties),

    ii.   "Fault" shall include the sale of defective or non-conforming Deliverables, negligence, willful misconduct, or a breach of any legally imposed strict liability standard.

B.   **THE CONTRACTOR SHALL DEFEND (AT THE OPTION OF THE CITY), INDEMNIFY, AND HOLD THE CITY, ITS SUCCESSORS, ASSIGNS, OFFICERS, EMPLOYEES AND ELECTED OFFICIALS HARMLESS FROM AND AGAINST ALL INDEMNIFIED CLAIMS DIRECTLY ARISING OUT OF, INCIDENT TO, CONCERNING OR RESULTING FROM THE FAULT OF THE CONTRACTOR, OR THE CONTRACTOR'S AGENTS, EMPLOYEES OR SUBCONTRACTORS, IN THE PERFORMANCE OF THE CONTRACTOR'S OBLIGATIONS UNDER THE CONTRACT. NOTHING HEREIN SHALL BE DEEMED TO LIMIT THE RIGHTS OF THE CITY OR THE CONTRACTOR (INCLUDING, BUT NOT LIMITED TO, THE RIGHT TO SEEK CONTRIBUTION) AGAINST ANY THIRD PARTY WHO MAY BE LIABLE FOR AN INDEMNIFIED CLAIM.**

32.   <u>**INSURANCE**</u>: (reference Section 0400 for specific coverage requirements). The following insurance requirement applies. (Revised March 2013).

A.   <u>General Requirements</u>.

    i.   The Contractor shall at a minimum carry insurance in the types and amounts indicated in Section 0400, Supplemental Purchase Provisions, for the duration of the Contract, including extension options and hold over periods, and during any warranty period.

    ii.   The Contractor shall provide Certificates of Insurance with the coverages and endorsements required in Section 0400, Supplemental Purchase Provisions, to the City as verification of coverage prior to contract execution and within fourteen (14) calendar days after written request from the City. Failure to provide the required Certificate of Insurance may subject the Offer to disqualification from consideration for award. The Contractor must also forward a Certificate of Insurance to the City whenever a previously identified policy period has expired, or an extension option or hold over period is exercised, as verification of continuing coverage.

    iii.   The Contractor shall not commence work until the required insurance is obtained and until such insurance has been reviewed by the City. Approval of insurance by the City shall not relieve or decrease the liability of the Contractor hereunder and shall not be construed to be a limitation of liability on the part of the Contractor.

    iv.   The City may request that the Contractor submit certificates of insurance to the City for all subcontractors prior to the subcontractors commencing work on the project.

    v.   The Contractor's and all subcontractors' insurance coverage shall be written by companies licensed to do business in the State of Texas at the time the policies are issued and shall be written by companies with A.M. Best ratings of B+VII or better.

    vi.   The "other" insurance clause shall not apply to the City where the City is an additional insured shown on any policy. It is intended that policies required in the Contract, covering both the City and the Contractor, shall be considered primary coverage as applicable.

    vii.   If insurance policies are not written for amounts specified in Section 0400, Supplemental Purchase Provisions, the Contractor shall carry Umbrella or Excess Liability Insurance for any differences in amounts specified. If Excess Liability Insurance is provided, it shall follow the form of the primary coverage.

viii.   The City shall be entitled, upon request, at an agreed upon location, and without expense, to review certified copies of policies and endorsements thereto and may make any reasonable requests for deletion or revision or modification of particular policy terms, conditions, limitations, or exclusions except where policy provisions are established by law or regulations binding upon either of the parties hereto or the underwriter on any such policies.

ix.   The City reserves the right to review the insurance requirements set forth during the effective period of the Contract and to make reasonable adjustments to insurance coverage, limits, and exclusions when deemed necessary and prudent by the City based upon changes in statutory law, court decisions, the claims history of the industry or financial condition of the insurance company as well as the Contractor.

x.   The Contractor shall not cause any insurance to be canceled nor permit any insurance to lapse during the term of the Contract or as required in the Contract.

xi.   The Contractor shall be responsible for premiums, deductibles and self-insured retentions, if any, stated in policies. Self-insured retentions shall be disclosed on the Certificate of Insurance.

xii.   The Contractor shall provide the City thirty (30) calendar days' written notice of erosion of the aggregate limits below occurrence limits for all applicable coverages indicated within the Contract.

xiii.   The insurance coverages specified in Section 0400, Supplemental Purchase Provisions, are required minimums and are not intended to limit the responsibility or liability of the Contractor.

B.   <u>Specific Coverage Requirements: Specific insurance requirements are contained in Section 0400, Supplemental Purchase Provisions</u>

33.   **CLAIMS**: If any claim, demand, suit, or other action is asserted against the Contractor which arises under or concerns the Contract, or which could have a material adverse affect on the Contractor's ability to perform thereunder, the Contractor shall give written notice thereof to the City within ten (10) calendar days after receipt of notice by the Contractor. Such notice to the City shall state the date of notification of any such claim, demand, suit, or other action; the names and addresses of the claimant(s); the basis thereof; and the name of each person against whom such claim is being asserted. Such notice shall be delivered personally or by mail and shall be sent to the City and to the Austin City Attorney. Personal delivery to the City Attorney shall be to City Hall, 301 West 2nd Street, 4th Floor, Austin, Texas 78701, and mail delivery shall be to P.O. Box 1088, Austin, Texas 78767.

34.   **NOTICES**: Unless otherwise specified, all notices, requests, or other communications required or appropriate to be given under the Contract shall be in writing and shall be deemed delivered three (3) business days after postmarked if sent by U.S. Postal Service Certified or Registered Mail, Return Receipt Requested. Notices delivered by other means shall be deemed delivered upon receipt by the addressee. Routine communications may be made by first class mail, telefax, or other commercially accepted means. Notices to the Contractor shall be sent to the address specified in the Contractor's Offer, or at such other address as a party may notify the other in writing. Notices to the City shall be addressed to the City at P.O. Box 1088, Austin, Texas 78767 and marked to the attention of the Contract Administrator.

35.   **RIGHTS TO BID, PROPOSAL AND CONTRACTUAL MATERIAL**: All material submitted by the Contractor to the City shall become property of the City upon receipt. Any portions of such material claimed by the Contractor to be proprietary must be clearly marked as such. Determination of the public nature of the material is subject to the Texas Public Information Act, Chapter 552, Texas Government Code.

36.   **NO WARRANTY BY CITY AGAINST INFRINGEMENTS**: The Contractor represents and warrants to the City that: (i) the Contractor shall provide the City good and indefeasible title to the Deliverables and (ii) the Deliverables supplied by the Contractor in accordance with the specifications in the Contract will not infringe, directly or contributorily, any patent, trademark, copyright, trade secret, or any other intellectual property right of any kind of any third party; that no claims have been made by any person or entity with respect to the ownership or operation of the Deliverables and the Contractor does not know of any valid basis for any such claims. The Contractor shall, at its sole expense, defend,

indemnify, and hold the City harmless from and against all liability, damages, and costs (including court costs and reasonable fees of attorneys and other professionals) arising out of or resulting from: (i) any claim that the City's exercise anywhere in the world of the rights associated with the City's' ownership, and if applicable, license rights, and its use of the Deliverables infringes the intellectual property rights of any third party; or (ii) the Contractor's breach of any of Contractor's representations or warranties stated in this Contract. In the event of any such claim, the City shall have the right to monitor such claim or at its option engage its own separate counsel to act as co-counsel on the City's behalf. Further, Contractor agrees that the City's specifications regarding the Deliverables shall in no way diminish Contractor's warranties or obligations under this paragraph and the City makes no warranty that the production, development, or delivery of such Deliverables will not impact such warranties of Contractor.

37. **CONFIDENTIALITY**: In order to provide the Deliverables to the City, Contractor may require access to certain of the City's and/or its licensors' confidential information (including inventions, employee information, trade secrets, confidential know-how, confidential business information, and other information which the City or its licensors consider confidential) (collectively, "Confidential Information"). Contractor acknowledges and agrees that the Confidential Information is the valuable property of the City and/or its licensors and any unauthorized use, disclosure, dissemination, or other release of the Confidential Information will substantially injure the City and/or its licensors. The Contractor (including its employees, subcontractors, agents, or representatives) agrees that it will maintain the Confidential Information in strict confidence and shall not disclose, disseminate, copy, divulge, recreate, or otherwise use the Confidential Information without the prior written consent of the City or in a manner not expressly permitted under this Agreement, unless the Confidential Information is required to be disclosed by law or an order of any court or other governmental authority with proper jurisdiction, provided the Contractor promptly notifies the City before disclosing such information so as to permit the City reasonable time to seek an appropriate protective order. The Contractor agrees to use protective measures no less stringent than the Contractor uses within its own business to protect its own most valuable information, which protective measures shall under all circumstances be at least reasonable measures to ensure the continued confidentiality of the Confidential Information.

38. **PUBLICATIONS**: All published material and written reports submitted under the Contract must be originally developed material unless otherwise specifically provided in the Contract. When material not originally developed is included in a report in any form, the source shall be identified.

39. **ADVERTISING**: The Contractor shall not advertise or publish, without the City's prior consent, the fact that the City has entered into the Contract, except to the extent required by law.

40. **NO CONTINGENT FEES**: The Contractor warrants that no person or selling agency has been employed or retained to solicit or secure the Contract upon any agreement or understanding for commission, percentage, brokerage, or contingent fee, excepting bona fide employees of bona fide established commercial or selling agencies maintained by the Contractor for the purpose of securing business. For breach or violation of this warranty, the City shall have the right, in addition to any other remedy available, to cancel the Contract without liability and to deduct from any amounts owed to the Contractor, or otherwise recover, the full amount of such commission, percentage, brokerage or contingent fee.

41. **GRATUITIES**: The City may, by written notice to the Contractor, cancel the Contract without liability if it is determined by the City that gratuities were offered or given by the Contractor or any agent or representative of the Contractor to any officer or employee of the City of Austin with a view toward securing the Contract or securing favorable treatment with respect to the awarding or amending or the making of any determinations with respect to the performing of such contract. In the event the Contract is canceled by the City pursuant to this provision, the City shall be entitled, in addition to any other rights and remedies, to recover or withhold the amount of the cost incurred by the Contractor in providing such gratuities.

42. **PROHIBITION AGAINST PERSONAL INTEREST IN CONTRACTS**: No officer, employee, independent consultant, or elected official of the City who is involved in the development, evaluation, or decision-making process of the performance of any solicitation shall have a financial interest, direct or indirect, in the Contract resulting from that solicitation. Any willful violation of this section shall constitute impropriety in office, and any officer or employee guilty thereof shall be subject to disciplinary action up to and including dismissal. Any violation of this provision, with the knowledge, expressed or implied, of the Contractor shall render the Contract voidable by the City.

43. **INDEPENDENT CONTRACTOR**: The Contract shall not be construed as creating an employer/employee relationship, a partnership, or a joint venture. The Contractor's services shall be those of an independent contractor. The Contractor agrees and understands that the Contract does not grant any rights or privileges established for employees of the City.

44. **ASSIGNMENT-DELEGATION**: The Contract shall be binding upon and enure to the benefit of the City and the Contractor and their respective successors and assigns, provided however, that no right or interest in the Contract shall be assigned and no obligation shall be delegated by the Contractor without the prior written consent of the City. Any attempted assignment or delegation by the Contractor shall be void unless made in conformity with this paragraph. The Contract is not intended to confer rights or benefits on any person, firm or entity not a party hereto; it being the intention of the parties that there be no third party beneficiaries to the Contract.

45. **WAIVER**: No claim or right arising out of a breach of the Contract can be discharged in whole or in part by a waiver or renunciation of the claim or right unless the waiver or renunciation is supported by consideration and is in writing signed by the aggrieved party. No waiver by either the Contractor or the City of any one or more events of default by the other party shall operate as, or be construed to be, a permanent waiver of any rights or obligations under the Contract, or an express or implied acceptance of any other existing or future default or defaults, whether of a similar or different character.

46. **MODIFICATIONS**: The Contract can be modified or amended only by a writing signed by both parties. No pre-printed or similar terms on any the Contractor invoice, order or other document shall have any force or effect to change the terms, covenants, and conditions of the Contract.

47. **INTERPRETATION**: The Contract is intended by the parties as a final, complete and exclusive statement of the terms of their agreement. No course of prior dealing between the parties or course of performance or usage of the trade shall be relevant to supplement or explain any term used in the Contract. Although the Contract may have been substantially drafted by one party, it is the intent of the parties that all provisions be construed in a manner to be fair to both parties, reading no provisions more strictly against one party or the other. Whenever a term defined by the Uniform Commercial Code, as enacted by the State of Texas, is used in the Contract, the UCC definition shall control, unless otherwise defined in the Contract.

48. **DISPUTE RESOLUTION**:

    A.   If a dispute arises out of or relates to the Contract, or the breach thereof, the parties agree to negotiate prior to prosecuting a suit for damages. However, this section does not prohibit the filing of a lawsuit to toll the running of a statute of limitations or to seek injunctive relief. Either party may make a written request for a meeting between representatives of each party within fourteen (14) calendar days after receipt of the request or such later period as agreed by the parties. Each party shall include, at a minimum, one (1) senior level individual with decision-making authority regarding the dispute. The purpose of this and any subsequent meeting is to attempt in good faith to negotiate a resolution of the dispute. If, within thirty (30) calendar days after such meeting, the parties have not succeeded in negotiating a resolution of the dispute, they will proceed directly to mediation as described below. Negotiation may be waived by a written agreement signed by both parties, in which event the parties may proceed directly to mediation as described below.

    B.   If the efforts to resolve the dispute through negotiation fail, or the parties waive the negotiation process, the parties may select, within thirty (30) calendar days, a mediator trained in mediation skills to assist with resolution of the dispute. Should they choose this option, the City and the Contractor agree to act in good faith in the selection of the mediator and to give consideration to qualified individuals nominated to act as mediator. Nothing in the Contract prevents the parties from relying on the skills of a person who is trained in the subject matter of the dispute or a contract interpretation expert. If the parties fail to agree on a mediator within thirty (30) calendar days of initiation of the mediation process, the mediator shall be selected by the Travis County Dispute Resolution Center (DRC). The parties agree to participate in mediation in good faith for up to thirty (30) calendar days from the date of the first mediation session. The City and the Contractor will share the mediator's fees equally and the parties will bear their own costs of participation such as fees for any consultants or attorneys they may utilize to represent them or otherwise assist them in the mediation.

49. **JURISDICTION AND VENUE**: The Contract is made under and shall be governed by the laws of the State of Texas, including, when applicable, the Uniform Commercial Code as adopted in Texas, V.T.C.A., Bus. & Comm. Code, Chapter 1, excluding any rule or principle that would refer to and apply the substantive law of another state or jurisdiction. All issues arising from this Contract shall be resolved in the courts of Travis County, Texas and the parties agree to submit to the exclusive personal jurisdiction of such courts. The foregoing, however, shall not be construed or interpreted to limit or restrict the right or ability of the City to seek and secure injunctive relief from any competent authority as contemplated herein.

50. **INVALIDITY**: The invalidity, illegality, or unenforceability of any provision of the Contract shall in no way affect the validity or enforceability of any other portion or provision of the Contract. Any void provision shall be deemed severed from the Contract and the balance of the Contract shall be construed and enforced as if the Contract did not contain the particular portion or provision held to be void. The parties further agree to reform the Contract to replace any stricken provision with a valid provision that comes as close as possible to the intent of the stricken provision. The provisions of this section shall not prevent this entire Contract from being void should a provision which is the essence of the Contract be determined to be void.

51. **HOLIDAYS:** The following holidays are observed by the City:

Holiday	Date Observed
New Year's Day	January 1
Martin Luther King, Jr.'s Birthday	Third Monday in January
President's Day	Third Monday in February
Memorial Day	Last Monday in May
Independence Day	July 4
Labor Day	First Monday in September
Veteran's Day	November 11
Thanksgiving Day	Fourth Thursday in November
Friday after Thanksgiving	Friday after Thanksgiving
Christmas Eve	December 24
Christmas Day	December 25

If a Legal Holiday falls on Saturday, it will be observed on the preceding Friday. If a Legal Holiday falls on Sunday, it will be observed on the following Monday.

52. **SURVIVABILITY OF OBLIGATIONS:** All provisions of the Contract that impose continuing obligations on the parties, including but not limited to the warranty, indemnity, and confidentiality obligations of the parties, shall survive the expiration or termination of the Contract.

53. **NON-SUSPENSION OR DEBARMENT CERTIFICATION:**

The City of Austin is prohibited from contracting with or making prime or sub-awards to parties that are suspended or debarred or whose principals are suspended or debarred from Federal, State, or City of Austin Contracts. By accepting a Contract with the City, the Vendor certifies that its firm and its principals are not currently suspended or debarred from doing business with the Federal Government, as indicated by the General Services Administration List of Parties Excluded from Federal Procurement and Non-Procurement Programs, the State of Texas, or the City of Austin.

54. **EQUAL OPPORTUNITY**

A. **Equal Employment Opportunity:** No Contractor, or Contractor's agent, shall engage in any discriminatory employment practice as defined in Chapter 5-4 of the City Code. No Offer submitted to the City shall be

considered, nor any Purchase Order issued, or any Contract awarded by the City unless the Offeror has executed and filed with the City Purchasing Office a current Non-Discrimination Certification. Non-compliance with Chapter 5-4 of the City Code may result in sanctions, including termination of the contract and the Contractor's suspension or debarment from participation on future City contracts until deemed compliant with Chapter 5-4.

B.   **Americans with Disabilities Act (ADA) Compliance:** No Contractor, or Contractor's agent, shall engage in any discriminatory practice against individuals with disabilities as defined in the ADA, including but not limited to: employment, accessibility to goods and services, reasonable accommodations, and effective communications.

55.   **BUY AMERICAN ACT-SUPPLIES (Applicable to certain Federally funded requirements)**

A.   Definitions. As used in this paragraph –

i.   "Component" means an article, material, or supply incorporated directly into an end product.

ii.   "Cost of components" means -

(1)   For components purchased by the Contractor, the acquisition cost, including transportation costs to the place of incorporation into the end product (whether or not such costs are paid to a domestic firm), and any applicable duty (whether or not a duty-free entry certificate is issued); or

(2)   For components manufactured by the Contractor, all costs associated with the manufacture of the component, including transportation costs as described in paragraph (1) of this definition, plus allocable overhead costs, but excluding profit. Cost of components does not include any costs associated with the manufacture of the end product.

iii.   "Domestic end product" means-

(1)   An unmanufactured end product mined or produced in the United States; or

(2)   An end product manufactured in the United States, if the cost of its components mined, produced, or manufactured in the United States exceeds 50 percent of the cost of all its components. Components of foreign origin of the same class or kind as those that the agency determines are not mined, produced, or manufactured in sufficient and reasonably available commercial quantities of a satisfactory quality are treated as domestic. Scrap generated, collected, and prepared for processing in the United States is considered domestic.

iv.   "End product" means those articles, materials, and supplies to be acquired under the contract for public use.

v.   "Foreign end product" means an end product other than a domestic end product.

vi.   "United States" means the 50 States, the District of Columbia, and outlying areas.

B.   The Buy American Act (41 U.S.C. 10a - 10d) provides a preference for domestic end products for supplies acquired for use in the United States.

C.   The City does not maintain a list of foreign articles that will be treated as domestic for this Contract; but will consider for approval foreign articles as domestic for this product if the articles are on a list approved by another Governmental Agency. The Offeror shall submit documentation with their Offer demonstrating that the article is on an approved Governmental list.

D.   The Contractor shall deliver only domestic end products except to the extent that it specified delivery of foreign end products in the provision of the Solicitation entitled "Buy American Act Certificate".

56.   **PROHIBITION OF BOYCOTT ISRAEL VERIFICATION**

Pursuant to Texas Government Code §2270.002, the City is prohibited from contracting with any "company" for goods or services unless the following verification is included in this **Contract**.

A.   For the purposes of this Section only, the terms "company" and "boycott Israel" have the meaning assigned by Texas Government Code §2270.001.

B.   If the **Principal Artist** qualifies as a "company", then the **Principal Artist** verifies that he:
   i.   does not "boycott Israel"; and
   ii.   will not "boycott Israel" during the term of this **Contract**.

C.   The **Principal Artist's** obligations under this Section, if any exist, will automatically cease or be reduced to the extent that the requirements of Texas Government Code Chapter 2270 are subsequently repealed, reduced, or declared unenforceable or invalid in whole or in part by any court or tribunal of competent jurisdiction or by the Texas Attorney General, without any further impact on the validity or continuity of this **Contract**.

CITY OF AUSTIN
PURCHASING OFFICE
SUPPLEMENTAL PURCHASE PROVISIONS

The following Supplemental Purchasing Provisions apply to this solicitation:

1. **EXPLANATIONS OR CLARIFICATIONS:** (reference paragraph 5 in Section 0200)

    All requests for explanations or clarifications must be submitted in writing to the Purchasing Office by email to Sai.Xoomsai@austintexas.gov or Daniel.Dellemonache@austintexas.gov by end of day 12/12/2017.

2. **INSURANCE:** Insurance is required for this solicitation.

    A. **General Requirements:** See Section 0300, Standard Purchase Terms and Conditions, paragraph 32, entitled Insurance, for general insurance requirements.

        i.   The Contractor shall provide a Certificate of Insurance as verification of coverages required below to the City at the below address prior to contract execution and within 14 calendar days after written request from the City. Failure to provide the required Certificate of Insurance may subject the Offer to disqualification from consideration for award

        ii. The Contractor shall not commence work until the required insurance is obtained and until such insurance has been reviewed by the City. Approval of insurance by the City shall not relieve or decrease the liability of the Contractor hereunder and shall not be construed to be a limitation of liability on the part of the Contractor.

        iii. The Contractor must also forward a Certificate of Insurance to the City whenever a previously identified policy period has expired, or an extension option or holdover period is exercised, as verification of continuing coverage.

        iv. The Certificate of Insurance, and updates, shall be mailed to the following address:

             City of Austin Purchasing Office
             P. O. Box 1088
             Austin, Texas 78767

             OR

             PURInsuranceCompliance@austintexas.gov

    B. **Specific Coverage Requirements:** The Contractor shall at a minimum carry insurance in the types and amounts indicated below for the duration of the Contract, including extension options and hold over periods, and during any warranty period. These insurance coverages are required minimums and are not intended to limit the responsibility or liability of the Contractor.

        i.   **Worker's Compensation and Employers' Liability Insurance:** Coverage shall be consistent with statutory benefits outlined in the Texas Worker's Compensation Act (Section 401). The minimum policy limits for Employer's Liability are $100,000 bodily injury each accident, $500,000 bodily injury by disease policy limit and $100,000 bodily injury by disease each employee.
             (1) The Contractor's policy shall apply to the State of Texas and include these endorsements in favor of the City of Austin:
                  (a) Waiver of Subrogation, Form WC420304, or equivalent coverage
                  (b) Thirty (30) days Notice of Cancellation, Form WC420601, or equivalent coverage

        ii. **Commercial General Liability Insurance:** The minimum bodily injury and property damage per occurrence are $500,000 for coverages A (Bodily Injury and Property Damage) and B (Personal and Advertising Injury).
             (1) The policy shall contain the following provisions:
                  (a) Contractual liability coverage for liability assumed under the Contract and all other Contracts related to the project.
                  (b) Contractor/Subcontracted Work.
                  (c) Products/Completed Operations Liability for the duration of the warranty period.

      (d)   If the project involves digging or drilling provisions must be included that provide Explosion, Collapse, and/or Underground Coverage.

    (2)   The policy shall also include these endorsements in favor of the City of Austin:

      (a)   Waiver of Subrogation, Endorsement CG 2404, or equivalent coverage

      (b)   Thirty (30) days Notice of Cancellation, Endorsement CG 0205, or equivalent coverage

      (c)   The City of Austin listed as an additional insured, Endorsement CG 2010, or equivalent coverage

iii.   **Business Automobile Liability Insurance:** The Contractor shall provide coverage for all owned, non-owned and hired vehicles with a minimum combined single limit of $500,000 per occurrence for bodily injury and property damage. Alternate acceptable limits are $250,000 bodily injury per person, $500,000 bodily injury per occurrence and at least $100,000 property damage liability per accident.

    (1)   The policy shall include these endorsements in favor of the City of Austin:

      (a)   Waiver of Subrogation, Endorsement CA0444, or equivalent coverage

      (b)   Thirty (30) days Notice of Cancellation, Endorsement CA0244, or equivalent coverage

      (c)   The City of Austin listed as an additional insured, Endorsement CA2048, or equivalent coverage.

C.   **Endorsements:** The specific insurance coverage endorsements specified above, or their equivalents must be provided. In the event that endorsements, which are the equivalent of the required coverage, are proposed to be substituted for the required coverage, copies of the equivalent endorsements must be provided for the City's review and approval.

3.   **TERM OF CONTRACT:**

A.   [The Contract shall commence upon execution, unless otherwise specified, and shall remain in effect for an initial term of 36 months. The Contract may be extended beyond the initial term for up to two additional 12 month periods at the City's sole option. If the City exercises any extension option, all terms, conditions, and provisions of the Contract shall remain in effect for that extension period, subject only to any economic price adjustment otherwise allowed under the Contract

B.   Upon expiration of the initial term or any period of extension, the Contractor agrees to hold over under the terms and conditions of this Contract for such a period of time as is reasonably necessary for the City to re-solicit and/or complete the deliverables due under this Contract. Any hold over period will not exceed 120 calendar days unless mutually agreed on by both parties in writing.

C.   Upon written notice to the Contractor from the City's Purchasing Officer or his designee and acceptance of the Contractor, the term of this contract shall be extended on the same terms and conditions for an additional period as indicated in paragraph A above.

4.   **INVOICES and PAYMENT:** (reference paragraphs 12 and 13 in Section 0300)

A.   Invoices shall contain a unique invoice number and the information required in Section 0300, paragraph 12, entitled "Invoices." Invoices received without all required information cannot be processed and will be returned to the vendor.

Invoices shall be mailed to the below address:

	City of Austin
Department	Aviation Department
Attn:	Account Payable

Address	3600 Presidential Blvd
City, State Zip Code	Austin, TX 78719

B.   The Contractor agrees to accept payment by either credit card, check or Electronic Funds Transfer (EFT) for all goods and/or services provided under the Contract. The Contractor shall factor the cost of processing credit card payments into the Offer. There shall be no additional charges, surcharges, or penalties to the City for payments made by credit card.

5. **LIVING WAGES:**

The City's Living Wage Program, Rule R161-17.14, is located at:
http://www.austintexas.gov/edims/document.cfm?id=277854

A.   The minimum wage required for all Contractor Employees (and all tiers of Subcontracting) directly assigned to this City Contract is $15.00 per hour, unless Published Wage Rates are included in this solicitation. In addition, the City may stipulate higher wage rates in certain solicitations in order to assure quality and continuity of service.

B.   The City requires Contractors submitting Offers on this Contract to provide a certification **(see the Living Wages Contractor Certification included in the Solicitation)** with their Offer certifying that all Contractor Employees (and all tiers of Subcontracting) directly assigned to this City Contract will be paid a minimum living wage equal to or greater than $15.00 per hour. The certification shall include a list of all Contractor Employees (and all tiers of Subcontracting) directly assigned to providing services under the resultant contract including their name and job title. The list shall be updated and provided to the City as necessary throughout the term of the Contract.

C.   The Contractor shall maintain throughout the term of the resultant contract basic employment and wage information for each employee as required by the Fair Labor Standards Act (FLSA).

D.   The Contractor shall provide to the Department's assigned Contract Manager with the first invoice, individual Employee Certifications for all Contractor Employees (and all tiers of Subcontracting) directly assigned to the contract. The City reserves the right to request individual Employee Certifications at any time during the contract term. Employee Certifications shall be signed by each Contractor Employee (and all tiers of Subcontracting) directly assigned to the contract. The Employee Certification   form   is   available   on-line   at https://www.austintexas.gov/financeonline/vendor_connection/index.cfm.

E.   Contractor shall submit employee certifications for Contractor Employees (and all tiers of Subcontracting) annually on the anniversary date of contract award with the respective invoice to verify that employees are paid the Living Wage throughout the term of the contract. The Employee Certification Forms shall be submitted for Contractor Employees (and all tiers of Subcontracting) added to the contract and/or to report any employee changes as they occur.

F.   The Department's assigned Contract Manager will periodically review the employee data submitted by the Contractor to verify compliance with this Living Wage provision. The City retains the right to review employee records required in paragraph C above to verify compliance with this provision.

6. **NON-COLLUSION, NON-CONFLICT OF INTEREST, AND ANTI-LOBBYING:**

A.   On June 14, 2018, the Austin City Council adopted Ordinance No. 20180614-056 replacing Chapter 2.7, Article 6 of the City Code relating to Anti-Lobbying and Procurement. The policy defined in this Code applies to Solicitations for goods and/or services requiring City Council approval under City

Charter Article VII, Section 15 (Purchase Procedures). The City requires Offerors submitting Offers on this Solicitation to certify that the Offeror has not in any way directly or indirectly had communication restricted in the ordinance section 2-7-104 during the No-Lobbying Period as defined in the Ordinance. The text of the City Ordinance is posted on the Internet at: https://assets.austintexas.gov/purchase/downloads/New_ALO_Ordinance_No_20180614-056.pdf and is also included in the Solicitation, Section 0200 V2, Solicitation Instructions June 26, 2018.

7. **WORKFORCE SECURITY CLEARANCE AND IDENTIFICATION (ID):**

   A. Contractors are required to obtain a certified criminal background report with fingerprinting (referred to as the "report") for all persons performing on the contract, including all Contractor, Subcontractor, and Supplier personnel (for convenience referred to as "Contractor's personnel").

   B. The report may be obtained by reporting to one of the below governmental entities, submitting to fingerprinting and requesting the report [requestors may anticipate a two-week delay for State reports and up to a four to six week delay for receipt of a Federal report.].

      i. Texas Department of Public Safety for any person currently residing in the State of Texas and having a valid Texas driver's license or photo ID card;
      ii. The appropriate governmental agency from either the U.S. state or foreign nation in which the person resides and holds either a valid U.S. state-issued or foreign national driver's license or photo ID card; or
      iii. A Federal Agency. A current Federal security clearance obtained from and certified by a Federal agency may be substituted.

   C. Contractor shall obtain the reports at least 30 days prior to any onsite work commencement. Contractor also shall attach to each report the project name, Contractor's personnel name(s), current address(es), and a copy of the U.S. state-issued or foreign national driver's license or photo ID card.

   D. Contractor shall provide the City a Certified Criminal Background Report affirming that Contractor has conducted required security screening of Contractor's personnel to determine those appropriate for execution of the work and for presence on the City's property. A list of all Contractor Personnel requiring access to the City's site shall be attached to the affidavit.

   E. Upon receipt by the City of Contractor's affidavit described in (D) above and the list of the Contractor's personnel, the City will provide each of Contractor's personnel a contractor ID badge that is required for access to City property that shall be worn at all times by Contractor's personnel during the execution of the work.

   F. The City reserves the right to deny an ID badge to any Contractor personnel for reasonable cause, including failure of a Criminal History background check. The City will notify the Contractor of any such denial no more than twenty (20) days after receipt of the Contractor's reports. Where denial of access by a particular person may cause the Contractor to be unable to perform any portion of the work of the contract, the Contractor shall so notify the City's Contract Manager, in writing, within ten (10) calendar days of the receipt of notification of denial.

   G. Contractor's personnel will be required to wear the ID badge at all times while on the work site. Failure to wear or produce the ID badge may be cause for removal of an individual from the work site, without regard to Contractor's schedule. Lost ID badges shall be reported to the City's Contract Manager. Contractor shall reimburse the City for all costs incurred in providing additional ID badges to Contractor Personnel.

   H. ID badges to enter and/or work on the City property may be revoked by the City at any time. ID badges must be returned to the City at the time of project completion and acceptance or upon removal of an individual from the work site.

I.   Contractor is not required to obtain reports for delivery personnel, including but not limited to FedEx, UPS, Roadway, or other materials delivery persons, however all delivery personnel must present company/employer-issued photo ID and be accompanied by at least one of Contractor's personnel at all times while at the work site.

J.   The Contractor shall retain the reports and make them available for audit by the City during regular business hours (reference paragraph 17 in Section 0300, entitled Right to Audit).

K.   Airport Security Requirements

i.   Access to any security or emergency documents must be approved by the Deparment of Aviation (DOA) Security Manager. Due to the ever changing environment of Airport security, requirements may change at any time.

SENSITIVE SECURITY INFORMATION must be protected at all times.

WARNING: This document contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this document may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the TSA or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For US government agencies public disclosure is governed by 5 U.S.C. 552 and CFR part 15 and 1520.

ii.   RESTRICTED AREAS ACCESS POLICIES

a.   Escorted Access: For this project Individuals will submit to a fingerprint-based ten-year criminal history records check (CHRC) and Security Threat Assessment (STA). If the process confirms no disqualifying criminal offenses, the DOA Security and ID Office will allow access, as approved by the Security Manager, to security areas and security documents. The Department of Aviation will provide escort services as part of this project as needed. Requests for access must be submitted in writing in advanced to the Security Manager so work can be scheduled accordingly.

b.   Telecommunication / Electrical / Maintenance Room Access:

- The DOA Information Systems Division will approve access into DOA telecommunication rooms.
- The DOA Building Maintenance Division will approve access into electrical and/or maintenance rooms.
- A DOA employee will accompany and escort individuals needing access to these areas. Requests for escorts must be made at least three (3) working days in advance of the event through the Project Manager and/or at the Work Coordination Meetings.

c.   The following procedures will be followed for approved parking:

- The Contractor must contact Airport Communications (530-2242) to advise they are arriving at the terminal, or have arrived at their approved parking location. DOA Security Supervisor or designee will be dispatched to meet at the designated parking location.
- DOA security representative will inspect the vehicle and apply a distinctive sticker to the vehicle window to indicate that the vehicle has been inspected and authorized to be parked at that location.
- Under no circumstances will the Contractors vehicle operator leave the vehicle prior to security inspection.

iii. SECURITY CLEARANCE PROCEDURES

a. The Contractor should allow 7-10 days for completion of security screening processing. Contact DOA Security and ID at 512-530-6360 for business hours.

b. The following procedures will be followed to obtain security clearance:

- Contract applicant will complete, sign the Personal Information Form, and present two forms of identification.

- Contract applicant will read and sign the Criminal History Records Check/Disqualifying Criminal Offenses statement/form.

- The Contractor will submit to an FBI fingerprint-based criminal history records check and a TSA Security Threat Assessment (STA).

- Non-U.S. citizen proposers will provide governmental proof of work authorization and an Aviation Department Documentation Verification Form reviewed and stamped by Immigration and Customs Enforcement personnel located on the ground level of the terminal building.

8. **INTERLOCAL PURCHASING AGREEMENTS:** (applicable to competitively procured goods/services contracts).

A. The City has entered into Interlocal Purchasing Agreements with other governmental entities, pursuant to the Interlocal Cooperation Act, Chapter 791 of the Texas Government Code. The Contractor agrees to offer the same prices and terms and conditions to other eligible governmental agencies that have an interlocal agreement with the City.

B. The City does not accept any responsibility or liability for the purchases by other governmental agencies through an interlocal cooperative agreement.

9. **OWNERSHIP AND USE OF DELIVERABLES:** The City shall own all rights, titles, and interests throughout the world in and to the Deliverables.

A. **Patents:** As to any patentable subject matter contained in the Deliverables, the Contractor agrees to disclose such patentable subject matter to the City. Further, if requested by the City, the Contractor agrees to assign and, if necessary, cause each of its employees to assign the entire right, title, and interest to specific inventions under such patentable subject matter to the City and to execute, acknowledge, and deliver and, if necessary, cause each of its employees to execute, acknowledge, and deliver an assignment of letters patent, in a form to be reasonably approved by the City, to the City upon request by the City.

B. **Copyrights:** As to any Deliverable containing copyrighted subject matter, the Contractor agrees that upon their creation, such Deliverables shall be considered as work made-for-hire by the Contractor for the City and the City shall own all copyrights in and to such Deliverables, provided however, that nothing in this Paragraph 36 shall negate the City's sole or joint ownership of any such Deliverables arising by virtue of the City's sole or joint authorship of such Deliverables. Should by operation of law, such Deliverables not be considered work made-for-hire, the Contractor hereby assigns to the City (and agrees to cause each of its employees providing services to the City hereunder to execute, acknowledge, and deliver an assignment to the City of Austin) all worldwide right, title, and interest in and to such Deliverables. With respect to such work made-for-hire, the Contractor agrees to execute, acknowledge and deliver and cause each of its employees providing services to the City hereunder

to execute, acknowledge, and deliver a work-for-hire agreement, in a form to be reasonably approved by the City, to the City upon delivery of such Deliverables to the City or at such other time as the City may request.

Notwithstanding the foregoing, Beyond20 will at all times be the sole owner of the Beyond20 Properties. ("Beyond20 Properties" means any Training Materials or Training Services, software, methodologies, techniques, tools, algorithms, and know-how that are used by Beyond20 in providing the Services and that do not constitute General Skills.)

C. **Additional Assignments:** The Contractor further agrees to, and if applicable, cause each of its employees to execute, acknowledge, and deliver all applications, specifications, oaths, assignments, and all other instruments which the City might reasonably deem necessary in order to apply for and obtain copyright protection, mask work registration, trademark registration and/or protection, letters patent, or any similar rights in any and all countries and in order to assign and convey to the City, its successors, assigns, and nominees, the sole and exclusive right, title, and interest in and to the Deliverables, The Contractor's obligations to execute acknowledge, and deliver (or cause to be executed, acknowledged, and delivered) instruments or papers such as those described in this Paragraph 36 A., B., and C. shall continue after the termination of this Contract with respect to such Deliverables. In the event the City should not seek to obtain copyright protection, mask work registration or patent protection for any of the Deliverables, but should arise to keep the same secret, the Contractor agrees to treat the same as Confidential Information under the terms of Paragraph above.

10. **CONTRACT MANAGER:** The following person is designated as Contract Manager, and will act as the contact point between the City and the Contractor during the term of the Contract:

Diana Heath
_____

Diana.Heath@austintexas.gov
_____

(512) 530-6341
_____

*Note: The above listed Contract Manager is not the authorized Contact Person for purposes of the **NON-COLLUSION, NON-CONFLICT OF INTEREST, AND ANTI-LOBBYING Provision** of this Section; and therefore, contact with the Contract Manager is prohibited during the no contact period.

SECTION 0401

Supplemental Purchase Provision –

Cloud Computing Requirements

Introduction

Cloud services can be highly beneficial when properly implemented in appropriate circumstances, but they are not the answer to every IT need. Cloud services can pose their own special risks, as can any powerful and innovative service delivery model. The Department of Aviation should examine all the issues relevant to their data and circumstances before determining whether and how to implement any cloud solution.
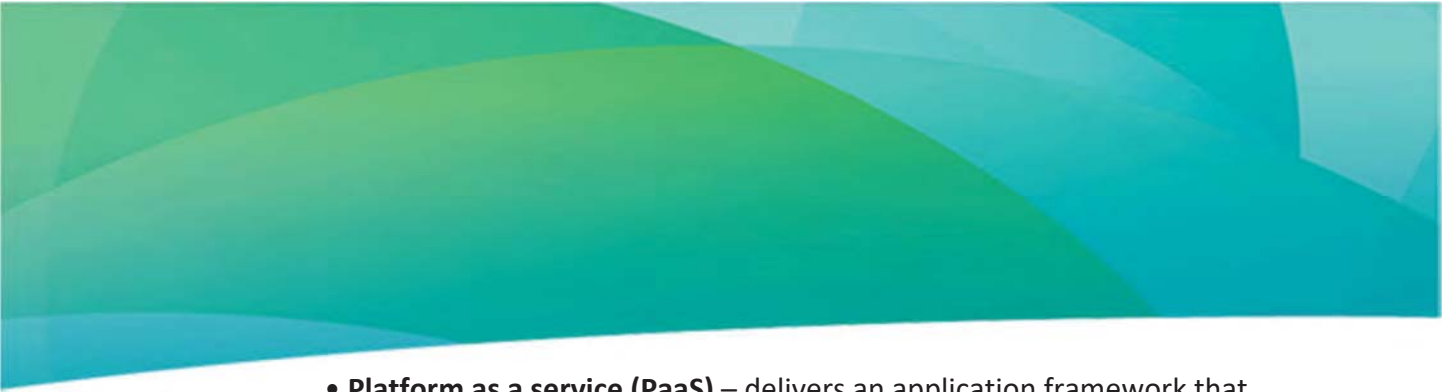
There are currently three different deployment models for cloud: public cloud, private cloud, and hybrid cloud.

• In a **public cloud**, the provider delivers common IT capability in a shared environment with great scalability. Demand from multiple customers with similar requirements are pooled together to optimize physical resources. Access is via an on-demand public network capability, such as the Internet.

• In a **private cloud**, IT resources are dedicated and customized with the capabilities, resources, and administration required by a specific organization. Access is generally through a secured or managed network. Private clouds require a data center location, IT physical resources, virtualization, and operations team support. A virtual private cloud is characterized by having a specific capacity in a public cloud carved out and dedicated to a particular organization and made available through a secured, managed virtual network.

• In a **hybrid cloud**, the provider blends both private and public cloud features together, with combination preferences usually driven by a particular market niche or consumer group based on an application or system that has partial needs for highly secure or non-virtual resources.

Types of services provided through the cloud include

• **Software as a service (SaaS)** – delivers applications, such as email, customer relationship management, and collaboration software.

• **Platform as a service (PaaS)** – delivers an application framework that supports design and development, testing, deployment, and hosting. PaaS enables organizations to develop custom applications on one platform, but then easily deploy to many hosting environments that support the same platform based on various pricing and service level agreement (SLA) models supported by the instance of that platform environment.

• **Infrastructure as a service (IaaS)** – delivers computing hardware, storage, networking, and other managed services such as backup, monitoring and virtual private network (VPN).

Requirements

The following are requirements in concern to Cloud Computing Services for the Department of Aviation (DOA).

Data Location

The Contractor shall provide its Services to the City of Austin, Department of Aviation (DOA) and its end users solely from data centers in the U.S. Storage of DOA Data at rest shall be located solely in data centers in the U.S. The Contractor shall not allow its personnel or contractors to store DOA Data on portable devices, including personal computers, except for devices that are used and kept only at its U.S. data centers. The Contractor may provide technical user support on a 24/7 basis using a support in other countries in order to provide round-the-clock support, unless otherwise prohibited in this contract.

Data

Data Ownership: The DOA will own all right, title and interest in its data that is related to the services provided by this contract. The Contractor shall not access DOA user accounts or DOA data, except (1) in the course of data center operations, (2) in response to service or technical issues, (3) as required by the express terms of this contract, or (4) at the DOA's written request.

Data Protection: Protection of personal privacy and data shall be an integral part of the business activities of the Contractor to ensure there is no inappropriate or unauthorized use of DOA information at any time. To this end, the Contractor shall safeguard the confidentiality, integrity and availability of DOA information and comply with the following conditions:

- The Contractor shall implement and maintain appropriate administrative, technical and organizational security measures to safeguard against unauthorized access, disclosure or theft of personal data and non-public data. Such security measures shall be in accordance with recognized industry practice and not less stringent than the measures the Contractor applies to its own personal data and non-public data of similar kind.

- All data obtained by the Contractor in the performance of this contract shall become and remain property of the DOA.

- All personal data shall be encrypted at rest and in transit with controlled access. Unless otherwise stipulated, the Contractor is responsible for encryption of the personal data. Any stipulation of responsibilities will identify specific roles and responsibilities and shall be included in the service level agreement (SLA), or otherwise made a part of this contract.

- Unless otherwise stipulated, the Contractor shall encrypt all non-public data at rest and in transit. The DOA shall identify data it deems as non-public data to the Contractor. The level of protection and encryption for all non-public data shall be identified and made a part of this contract.

- At no time shall any data or processes – that either belong to or are intended for the use of a DOA or its officers, agents or employees – be copied, disclosed or retained by the Contractor or any party related to the Contractor for subsequent use in any transaction that does not include the DOA.

- The Contractor shall not use any information collected in connection with the service issued from this proposal for any purpose other than fulfilling the service.

Compliance with Accessibility Standards: The Contractor shall comply with and adhere to Accessibility Standards of Section 508 Amendment to the Rehabilitation Act of 1973.
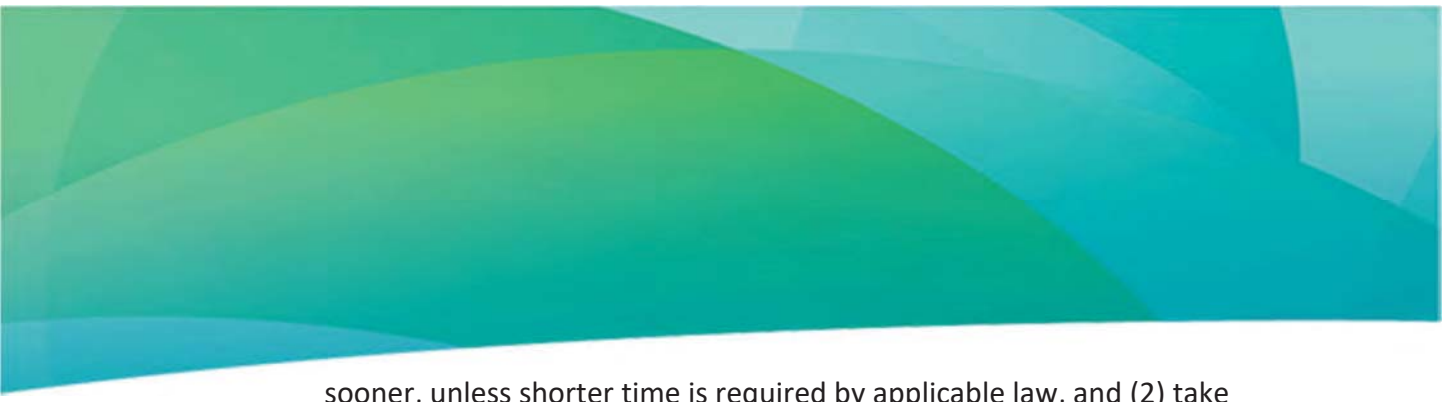
Security: The Contractor shall disclose its non-proprietary security processes and technical limitations to the DOA such that adequate protection and flexibility can be attained between the DOA and the Contractor.

Security in Compliance with Chapter 521 of the Texas Business and Commerce Code: Contractor shall comply with all requirements under Chapter 521 of the Texas Business and Commerce Code, including but not limited to being responsible for a program that protects against the unlawful use or disclosure of personal information collected or maintained in the regular course of business. The program shall include policies and procedures for the implementation of administrative, technical, and physical safeguards, and shall also address appropriate corrective action for events of any security breach and proper methods of destroying records containing sensitive personal information.

Security Incident or Data Breach Notification: The Contractor shall inform the DOA of any security incident or data breach.

- Incident Response: The Contractor may need to communicate with outside parties regarding a security incident, which may include contacting law enforcement, fielding media inquiries and seeking external expertise as mutually agreed upon, defined by law or contained in the contract. Discussing security incidents with the DOA should be handled on an urgent as-needed basis, as part of Contractor communication and mitigation processes as mutually agreed upon, defined by law or contained in the contract.

- Security Incident Reporting Requirements: The Contractor shall report a security incident to the appropriate DOA identified contact immediately as defined in the SLA.

- Breach Reporting Requirements: If the Contractor has actual knowledge of a confirmed data breach that affects the security of any DOA content that is subject to applicable data breach notification law, the Contractor shall (1) promptly notify the appropriate DOA identified contact within 24 hours or
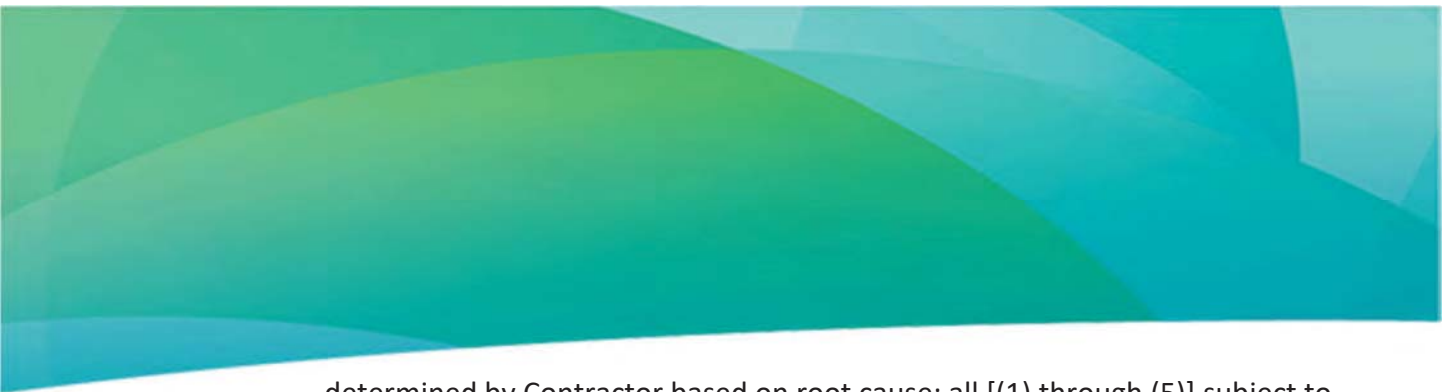
sooner, unless shorter time is required by applicable law, and (2) take commercially reasonable measures to address the data breach in a timely manner.

Breach Responsibilities: This section only applies when a data breach occurs with respect to personal data within the possession or control of Contractor.

- The Contractor, unless stipulated otherwise, shall immediately notify the appropriate DOA identified contact by telephone in accordance with the agreed upon security plan or security procedures if it reasonably believes there has been a security incident.

- The Contractor, unless stipulated otherwise, shall promptly notify the appropriate DOA identified contact within 24 hours or sooner by telephone, unless shorter time is required by applicable law, if it confirms that there is, or reasonably believes that there has been a data breach. The Contractor shall (1) cooperate with the DOA as reasonably requested by the DOA to investigate and resolve the data breach, (2) promptly implement necessary remedial measures, if necessary, and (3) document responsive actions taken related to the data breach, including any post-incident review of events and actions taken to make changes in business practices in providing the services, if necessary.

- Unless otherwise stipulated, if a data breach is a direct result of the Contractor's breach of its contract obligation to encrypt personal data or otherwise prevent its release, the Contractor shall bear the costs associated with (1) the investigation and resolution of the data breach; (2) notifications to individuals, regulators or others required by state law; (3) a credit monitoring service required by state (or federal) law; (4) establishing a website or a toll-free number and call center for affected individuals required by state law – all not to exceed the average per record per person cost calculated for data breaches in the United States (currently $201 per record/person) in the most recent Cost of Data Breach Study: Global Analysis published by the Ponemon Institute at the time of the data breach; and (5) complete all corrective actions as reasonably

determined by Contractor based on root cause; all [(1) through (5)] subject to this contract's limitation of liability.
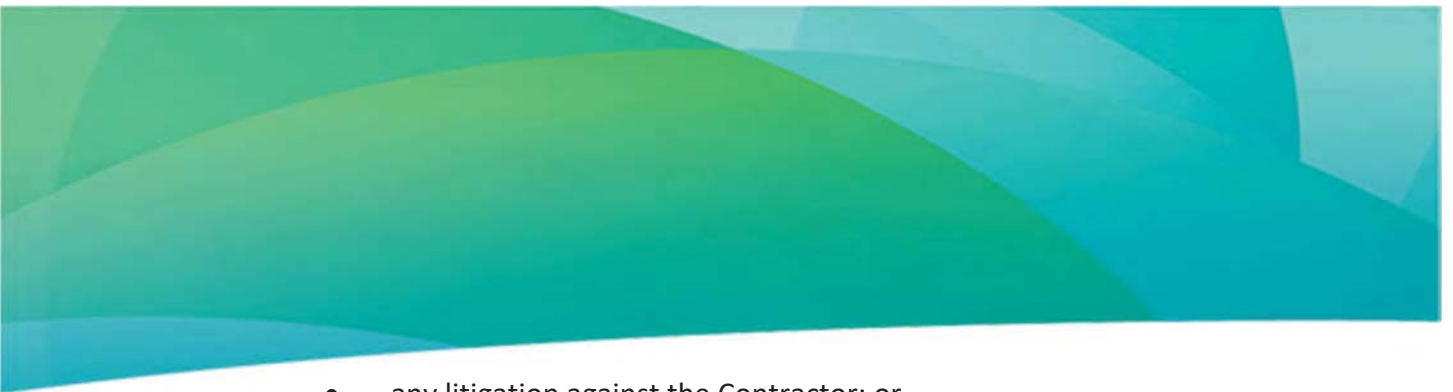
Business Continuity and Disaster Recovery: The Contractor shall provide a business continuity and disaster recovery plan upon request and ensure that the DOA's recovery time objective (RTO) of two hours is met.

Significant Event

The Contractor shall immediately notify the DOA's Information Systems Manager of any current or prospective "significant event" on an ongoing basis. All notifications shall be submitted in writing to the Information Systems Manager. As used in this provision, a "significant event" is any occurrence or anticipated occurrence which might reasonably be expected to have a material effect upon the Contractor's ability to meet its contractual obligations. Significant events may include but not be limited to the following:

- disposal of major assets;

- any major computer software conversion, enhancement or modification to the operating systems, security systems, and application software, used in the performance of this Contract;

- any significant termination or addition of provider contracts;

- the Contractor's insolvency or the imposition of, or notice of the intent to impose, a receivership, conservatorship or special regulatory monitoring, or any bankruptcy proceedings, voluntary or involuntary, or reorganization proceedings;

- strikes, slow-downs or substantial impairment of the Contractor's facilities or of other facilities used by the Contractor in the performance of this Contract;

- reorganization, reduction and/or relocation in key personnel;

- known or anticipated sale, merger, or acquisition;

- known, planned or anticipated stock sales;

- any litigation against the Contractor; or

- significant change in market share or product focus.

Audits and Records

Data Center Audit: The Contractor shall perform an independent audit of its data centers at least annually at its expense, and provide a redacted version of the audit report upon request. The Contractor may remove its proprietary information from the redacted version. A Service Organization Control (SOC) 2 audit report or approved equivalent sets the minimum level of a third-party audit.

Confidentiality

In order to provide the deliverables to the DOA, Contractor may require access to certain of the DOA's and/or its licensors' confidential information (including inventions, employee information, trade secrets, confidential know-how, confidential business information, and other information which the DOA or its licensors consider confidential) (collectively, "Confidential Information"). Contractor acknowledges and agrees that the Confidential Information is the valuable property of the DOA and/or its licensors and any unauthorized use, disclosure, dissemination, or other release of the Confidential Information will substantially injure the DOA and/or its licensors. The Contractor (including its employees, subcontractors, agents, or representatives) agrees that it will maintain the Confidential Information in strict confidence and shall not disclose, disseminate, copy, divulge, recreate, or otherwise use the Confidential Information without the prior written consent of the DOA or in a manner not expressly permitted under this Contract, unless the Confidential Information is required to be disclosed by law or an order of any court or other governmental authority with proper jurisdiction, provided the Contractor promptly notifies the DOA before disclosing such information so as to permit the DOA reasonable time to seek an appropriate protective order. The Contractor agrees to use protective measures no less stringent than the Contractor uses within its own business to protect its own most valuable information, which protective measures shall under all circumstances be at least reasonable measures to ensure the continued confidentiality of the Confidential Information.

Subcontractors

Work performed for the Contractor by a Subcontractor shall be pursuant to a written contract between the Contractor and Subcontractor. The terms of the subcontract may not conflict with the terms of the Contract, and shall contain provisions that:

- require that all deliverables to be provided by the Subcontractor be provided in strict accordance with the provisions, specifications and terms of the Contract.

- prohibit the Subcontractor from further subcontracting any portion of the Contract without the prior written consent of the DOA and the Contractor.

- require Subcontractors to submit all invoices and applications for payments, including any claims for additional payments, damages or otherwise, to the Contractor in sufficient time to enable the Contractor to include same with its invoice or application for payment to the DOA in accordance with the terms of the Contract;

- require that all Subcontractors obtain and maintain, throughout the term of their contract, insurance in the type and amounts specified for the Contractor, with the DOA being a named insured as its interest shall appear; and

- require that the Subcontractor indemnify and hold the DOA harmless to the same extent as the Contractor is required to indemnify the DOA.

The Contractor shall be fully responsible to the DOA for all acts and omissions of the Subcontractors just as the Contractor is responsible for the Contractor's own acts and omissions. Nothing in the Contract shall create for the benefit of any such Subcontractor any contractual relationship between the DOA and any such Subcontractor, nor shall it create any obligation on the part of the DOA to pay or to see to the payment of any moneys due any such Subcontractor except as may otherwise be required by law.

The Contractor shall pay each Subcontractor its appropriate share of payments made to the Contractor not later than ten (10) calendar days after receipt of payment from the DOA.

Austin-Bergstrom International Airport

Information Technology Service Management Software Solution

Section 0500 Statement of Work

City of Austin, Department of Aviation

Table of Contents

1. PURPOSE

The City of Austin, Department of Aviation (the Airport) is seeking proposals for an Information Technology Service Management Toolset (ITSM) software solution and implementation services to replace the existing Heat help desk system. This new solution will be implemented at the Austin-Bergstrom International Airport (ABIA). The ITSM solution requires modules that cover all aspects of the Information Technology Infrastructure Library v3-2011 (ITIL) processes for IT Service Management. The solution must provide fully integrated functionality across the following stages: Service Strategy, Service Design, Service Transition, Service Operation, and Continual Service Improvement. The solution must address all items above and within this scope of work.

2. BACKGROUND AND PROJECT OVERVIEW

The Airport Information Systems Division (IS) currently uses a subset of Ivanti Service Manager Tools, based on HEAT Software's ticket management system. It is considered a "Business Operational" system, defined as "contributing to efficient business operation but out of direct line of service to the customers." The primary user of the ticketing system is the Airport IS Service Desk. The current solution is an on-premise system, using Airport IS server hardware and enterprise software, including SQL. Server management functions are performed by IS staff.

Airport IS has recently concluded a project to define key ITSM processes and is currently implementing them. Procuring a proper software solution to assist IS with integration of the new processes is the identified next step in service management.

IS intends to procure a service management solution to support their transition into a service management organization. The purpose of this project is to partner with a vendor and implementer to:

a. Procure and implement a best-fit ITSM solution for the Airport.
b. Work with the IS team and their ITSM consulting team to implement existing and new processes, with a focus on: Service Request Fulfillment, Change Management, Problem Management, and Incident Management.
c. Deliver solution training, with delivery options for the IS staff and other stakeholders.
d. Provide software support and maintenance.

Although the current system is an on-premise solution, the Airport is willing to review alternate forms of hosting, but Cloud solutions must conform to the City's and Airport's Security standards. Vendors should provide all pricing and configuration information for all products proposed, including implementation, training, and other professional services, as IS intends to review both on-premise and cloud solutions.

3. REQUIRED PROJECT TIMELINE

This project supports the Airport's IS Division's ongoing efforts to become a Service-based organization to support all internal and airport clients. The Airport expects implementation of the IT Service Management Software Solution to be phased, based on implemented processes, but also upon vendor recommendations.

- ITSM solution fully functional by no later than 6 months after contract Notice to Proceed.

4. VENDOR MINIMUM QUALIFICATIONS

The ITSM Service Management Software Solution Contractor shall have been in the business of selling, designing, implementing, and maintaining ITSM solutions at other similar organizations for a minimum of five (5) years.

The Contractor shall hold current advisor, administrator and implementer certifications and/or training from the proposed software vendor. The Contractor shall service all equipment and software of the solution.

5. BASE SCOPE ELEMENTS AND SERVICES

A.   General Requirements

1. The Contractor shall provide support and maintenance of all modules installed including any 3rd party modules.

2. The Contractor shall provide the technical expertise to maintain, test and troubleshoot.

6. SUPPORTING SCOPE ELEMENTS

The Contractor shall perform the general scope of work described herein.

A. The Contractor shall provide project management and related services for the implementation of the ITSM Service Management Software Solution, as described above, through final system acceptance, coordinating with Airport program management services.

B. The Contractor shall be responsible for the implementation of the solution and shall provide the following services, including but not limited to:
   1. Project management and coordination.
   2. System design services.
   3. System installation, configuration, interface, migrations, and integration while working with the Airport consultant team.
   4. All required coordination with DOA representatives, other system vendors, Airport consultants, and project representatives.
   5. Solution testing.
   6. Solution training.

C. The Contractor shall prepare the necessary documents required for installing, testing, and bringing the ITSM Service Management Software Solution online. Such documents may include, but are not limited to:
   1. Project management and quality assurance plans
   2. System design plans/documents
   3. Component and system submittal documents
   4. Installation plans
   5. Testing plans
   6. System user documentation, including process, procedures and recommended policies
   7. Final setup and configuration documents

D. The Contractor shall coordinate with Airport Project Manager or designated representative and the Airport's consultants to ensure the installed system meets the required goals of the Airport.

E. The Contractor shall supply all software necessary for the ITSM Service Management Software Solution to function as specified. The Airport will procure required hardware and server licensing, if necessary. The Contract shall provide specifications of required hardware to be procured by the Airport.

F. The Contractor shall assign a project manager that directly reports to the Airport's Project Manager to support the specific coordination requirements associated with the installation of the ITSM Service Management Software Solution.

G. The Contractor shall verify system operability and proper installation via completion of all required test plans and use cases. Beyond20 will conduct unit testing of configurations, but the Airport shall also conduct user acceptance testing as part of the engagement.

H. Any maintenance work performed on the system (on-premise or Cloud-based) shall be performed during the Airport's designated maintenance window which is defined as between the hours of 12:00 AM and 4:00 AM.

7. SECURITY, CONFIDENTIALITY, AND NETWORK DATA SECURITY REQUIREMENTS

A. Contractor on-site staff and remote staff shall meet all local and national security requirements and comply with all laws and regulations that are otherwise legally required to work at the airport. Refer to Exhibit A: Airport Security Requirements for more detail.

B. Contractor on-site staff shall meet the minimum Airport security requirements and be capable of obtaining and maintaining a current valid SIDA badge at Aviation Department.

C. Contractor's on-site and remote staff shall sign a non-disclosure agreement and keep the details of Aviation Department confidential. Failure to sign or abide by the non-disclosure agreement shall be grounds for contract cancellation.

D. Remote access shall meet Aviation Department security requirements. Contractor shall notify Aviation Department within 24 hours of a termination or resignation of support staff.

E. All materials and information provided or made available to the Contractor by the City or while working on this Contract for the Airport shall be regarded as confidential information in accordance with Federal law, State law, and ethical standards. The Contractor shall take all necessary steps to safeguard the confidentiality of such materials or information. The Contractor shall ensure that its employees and Subcontractors associated with this contract abide by the confidentiality requirements of the Contract. The Contractor certifies that their employees, agents and Subcontractors, prior to working on this project, will have signed the Airport's Confidentiality Agreement.

F. The Airport will provide security for gaining entry and access to its sites. As some program and individual data is of a highly sensitive nature and cannot be removed from the work location, the Contractor shall be responsible for sanitizing, i.e., removing or redacting, any such data before its removal.

G. The Contractor shall be responsible for its Subcontractors' actions and shall be held liable for any data corruption caused by the Contractor or its Subcontractors.

CHERWELL END-USER SUBSCRIPTION AGREEMENT

THIS END-USER SUBSCRIPTION AGREEMENT ("EUSA"), TOGETHER WITH ANY APPLICABLE CHERWELL ORDER CONFIRMATION FORM THAT REFERENCES THIS EUSA (COLLECTIVELY, THE "AGREEMENT"), IS BETWEEN CHERWELL SOFTWARE, LLC, A DELAWARE LIMITED LIABILITY COMPANY ("CHERWELL"), AND THE CUSTOMER IDENTIFIED ON THE ORDER CONFIRMATION FORM ("CUSTOMER"). THIS AGREEMENT CONSTITUTES THE ENTIRE AGREEMENT BETWEEN CUSTOMER AND CHERWELL REGARDING THE CHERWELL SOFTWARE PRODUCTS ("LICENSED SOFTWARE") AND THE MAINTENANCE AND SUPPORT AND PROFESSIONAL SERVICES THAT ARE LISTED ON THE ORDER CONFIRMATION FORM. BY INSTALLING OR USING THE LICENSED SOFTWARE, CUSTOMER ACKNOWLEDGES THAT IT HAS READ AND AGREES TO ALL OF THE TERMS AND CONDITIONS CONTAINED IN THIS AGREEMENT.

1.   GRANT OF LICENSE AND SUBSCRIPTION

1.1   Subscription License. The Licensed Software, which includes all configurable and executable application content or "Blueprints," is licensed to Customer for use subject to the terms of this Agreement. Cherwell hereby grants to Customer and Customer fully accepts, upon delivery, a nonexclusive, non-transferable right to access and use only the executable version (no source code) of the Licensed Software, during the term of the Subscription Service, as described below (the "Subscription Service"). This is not a perpetual use license; rather, Customer is using the Licensed Software pursuant to the Subscription Service and for a limited duration. Customer is allowed only the number of concurrent users of the Licensed Software as shown on the Cherwell Order Confirmation Form. If Customer wishes to expand the number of authorized concurrent users covered by the license, Customer can purchase additional user licenses. Customer's authorized concurrent users of the Licensed Software can include Customer, its subsidiaries and affiliates, and their employees and authorized representatives, agents and contractors. Customer may install copies of the Licensed Software in non-production environments, for purposes of testing, development or disaster recovery, provided, however, that such copies cannot be used for production purposes and there cannot be more than one installation of the Licensed Software in a production environment. In no event shall the number of concurrent users in a production environment exceed the authorized concurrent users covered by the license.

1.2   CHERWELL ASSET MANAGEMENT

1.2.1   If purchased by Customer, the term Licensed Software shall include the Cherwell software product known as Cherwell Asset Management ("CAM Software"), which includes, but is not limited to: (a) the Cherwell proprietary application database ("Cherwell Software Identification Database™" or "CSID™") and the data accessed by and/or contained therein, (b) the Logi Analytics, Inc. proprietary software product known as "Logi Info Server", (c) the reports generated by use of CAM Software, and (d) CAM Software product documentation. Notwithstanding anything to the contrary in this Agreement, Customer shall have the right to terminate its subscription license of the CAM Software after one year from the Effective Date (as defined below). For the avoidance of doubt, termination of the subscription license of the CAM Software shall not terminate Customer's subscription license of the other Licensed Software.

1.2.2   With regard to CAM Software, Customer acknowledges and agrees that it may install a copy of the CAM Software on a network server(s), provided that Customer acquires and dedicates a license for each computer workstation on the network(s) on which the CAM Software will be used. The CAM Software is "used" when it is loaded in temporary or permanent memory of a computer. In addition, Cherwell grants to Customer a limited, personal, non-transferable and non-exclusive right to use the CAM Software in connection with a server, application server, or desktop application virtualization technology. This includes but is not limited to Citrix®, Microsoft Terminal Server®, or VMWare® technologies that are capable of creating multiple virtual machines or sessions on which the CAM Software can be run. Customer must acquire and dedicate a license for each such machine, virtual machine, or session running a separate instance of the CAM Software.

1.2.3   The CSID may be installed on servers solely for use in conjunction with Customer's licensed copies of the CAM Software, in accordance with the product documentation.

1.3   **Subscription Service Term.** This Agreement is effective as of the earlier of the date Customer first uses or installs the Licensed Software or the date set forth on the Cherwell Order Confirmation Form (the "Effective Date").   Customer's right to use the Licensed Software continues until this Agreement is terminated or the Subscription Service expires.   The Subscription Service is offered on no less than an annual basis and will commence and be invoiced in advance of each annual period to Beyond20... Subscription fees increase as Customer adds additional concurrent user licenses.   Either party may terminate this Agreement upon written notice to the other party if the other party fails to cure a material breach of this Agreement within thirty (30) days of written notice of the breach from the terminating party.   Upon any termination, Customer agrees to remove all Licensed Software from its computers, destroy all copies of the Licensed Software, and, upon request from Cherwell, certify in writing its compliance.   Upon termination by Customer for an uncured breach by Cherwell, Cherwell will pay Customer a pro rata refund of any prepaid but unused Subscription Fees.

1.4   **Intellectual Property Rights.** The Licensed Software is protected by copyright and other intellectual property laws.   Cherwell retains all rights, title and interest in and to the Licensed Software. Customer agrees that this is a license only and that no title passes to Customer.   If Customer makes or installs copies of the Licensed Software as provided in this Agreement, the original and all copies of the Licensed Software may not leave Customer's control and are owned by Cherwell.   Customer retains all rights to its data.

1.5   **Restrictions.** To the maximum extent permitted by applicable law, Customer may not resell or otherwise transfer for value the Licensed Software without the written consent of Cherwell.   Customer may not export, ship, transmit, or re-export the Licensed Software in violation of any applicable law or regulation, including, without limitation, the Export Administration Regulations issued by the United States Department of Commerce and the United States trade embargoes and economic sanctions administered by the U.S. Treasury Department, Office of Foreign Assets Control, or any such similar law or regulation issued by such other governmental entity which may have jurisdiction over such export.   Customer agrees not to: (i) modify, decompile, disassemble or reverse engineer the object code portions of the Licensed Software; (ii) distribute, rent, lease or lend the Licensed Software; or (iii) use the Licensed Software except as expressly permitted under this Agreement.

2.   **INDEMNIFICATION**
2.1   Cherwell shall defend, indemnify and hold Customer harmless against all third party claims, suits, proceedings, costs, damages, losses and expenses (including reasonable attorneys' fees), and judgments incurred, claimed or sustained by Customer arising out of or related to any allegation that any portion of the Licensed Software (including any updates, error corrections, or upgrades thereto), when used solely in the manner and for the purpose for which it was licensed hereunder, violates any patent, copyright, trade secret, trademark, or other third party intellectual property right.   If a claim is filed in a court or other administrative proceeding seeking to enjoin the use of the Licensed Software, Cherwell shall either: (i) at Cherwell's cost, procure for Customer the right to continue to use the relevant portion of the Licensed Software; (ii) replace, at Cherwell's cost, the relevant portion of the Licensed Software with a substitute product that functions substantially in accordance with the applicable specifications for that portion of the Licensed Software; or (iii) at Cherwell's cost, modify the Licensed Software so that it does not infringe or misappropriate, provided that the Licensed Software, as modified, continues to perform substantially in accordance with the applicable specifications.

2.2   Cherwell's indemnification obligation pursuant to the above shall not apply to the extent any infringement claim is found to be caused by (i) Customer's use of the Licensed Software in a manner that is not provided for under this Agreement or Cherwell's user documentation; or (ii) Customer's use, operation or combination of all or any component or portion of the Licensed Software with all or any portion of other software, equipment or systems not provided or required by Cherwell. As a condition precedent to any liability of Cherwell, if Customer receives notice of any infringement claims for which indemnification may be available under the above, Customer must promptly notify Cherwell in writing of the infringement claim.

2.3   Cherwell will have the right to control the defense, select counsel, and direct the course of resolution, including settlement of any infringement claim (but only if the settlement does not include an admission of liability by Customer, does not involve more than the payment of money and grants Customer a full and unconditional release from all liability with respect to the claim).   In addition to the defense provided by Cherwell, Customer may elect to retain its own counsel, but Cherwell will not be responsible for any fees or expenses of such counsel.

3.   WARRANTIES AND DISCLAIMERS

3.1   Limited Warranties. Each party represents and warrants to the other that it has the legal power to enter into this Agreement. Cherwell further represents and warrants that: (i) it has the right to grant to Customer the license to use the Licensed Software as set forth in this Agreement without violating any rights of any third party and that, to the best of Cherwell's knowledge, the Licensed Software does not infringe or otherwise violate any intellectual property rights of any third party; (ii) the Licensed Software shall operate in material compliance with Cherwell's user documentation; (iii) all services provided by Cherwell pursuant to this Agreement relating to the Licensed Software will be performed in a timely and professional manner, by qualified and skilled individuals, and in conformity with standards generally accepted in Cherwell's industry; and (iv) the Licensed Software shall be delivered free of any virus or otherwise malicious code, or any code or command intended to bring down the Licensed Software or Customer's computers/networks automatically or upon command or otherwise impair their use.

3.2   Limited Remedy. In the event of any breach of warranty, Customer's sole and exclusive remedy shall be for Cherwell to either correct or replace, at no additional charge to Customer, any portion of the Licensed Software or services found to be defective or, if Cherwell is unable to correct or replace the defect, refund any prepaid but unused Subscription Service fees paid by Customer; and in the event Cherwell introduces any virus or such disabling code or commands into the Licensed Software or any of Customer's equipment, make commercially reasonable efforts to restore any and all data or programming lost by Customer as a result of such virus or disabling code.

3.3   Disclaimer. TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, THE WARRANTIES SET FORTH IN SECTION 3 ARE EXCLUSIVE AND IN LIEU OF ALL OTHER WARRANTIES, ORAL OR WRITTEN, EXPRESSED OR IMPLIED.   CHERWELL DOES NOT WARRANT THAT THE OPERATION OF THE LICENSED SOFTWARE WILL BE UNINTERRUPTED OR ERROR FREE. EXCEPT AS SET FORTH IN THIS SECTION 3, CHERWELL MAKES NO WARRANTY OR REPRESENTATION, EITHER EXPRESSED OR IMPLIED, WITH RESPECT TO THE LICENSED SOFTWARE, ITS QUALITY, PERFORMANCE, MERCHANTABILITY, OR FITNESS FOR A PARTICULAR PURPOSE.

4.   LIMITATION OF LIABILITY; EXCLUSION OF DAMAGES

4.1   Limitation of Liability. To the maximum extent permitted by applicable law and except for Customer's payment obligations under this Agreement and Cherwell's obligation to indemnify Customer under Section 2, each party's entire liability under this Agreement shall be limited to three times the amount paid by Customer for the Subscription Service during the most recent twenty-four (24) month period, which shall not include any amount paid for related or Professional Services.

This limitation of liability shall not affect Cherwell's indemnification obligations hereunder, warranty claims, or claims not covered under an insurance policy.

4.2   Exclusion of Consequential and Related Damages.   TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, IN NO EVENT SHALL EITHER PARTY BE LIABLE TO THE OTHER FOR LOST PROFITS, LOSS OF USE OR INDIRECT, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES, WHETHER IN CONTRACT, TORT OR ANY OTHER THEORY OF LIABILITY, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGES, EXCEPT TO THE EXTENT THAT ANY THIRD PARTY CLAIM SUBJECT TO INDEMNIFICATION UNDER SECTION 2 INCLUDES SUCH DAMAGES.

5.   MAINTENANCE AND SUPPORT AND SERVICES

5.1   General. The Subscription Service includes Maintenance and Support of the Licensed Software. Failure to pay any amount due under this Agreement may result in suspension of Maintenance and Support.   If Maintenance and Support is interrupted as a result of expiration or termination, Customer may be charged a reinstatement fee equal to the cost of Maintenance and Support for the period from the date of expiration or termination to the date of renewal.

5.2   Maintenance. "Maintenance" entitles Customer to receive updates, upgrades, patches, bug fixes and new releases or versions of the Licensed Software, including updated documentation, as Cherwell may provide from time to time without requirement of a separate license agreement, and without additional charge other than payment of the Subscription fee.

5.3   Support. Where provided by and purchased from Cherwell, "Support" entitles Customer to technical assistance with Customer's ongoing use of the Licensed Software, 24 hours a day, 7 days a week. Cherwell will provide support for the most current version of the Licensed Software and one prior version, including interim releases between the two versions; for example, upon release of version 5.x Cherwell will support version 5.x and 4.x. Cherwell may provide limited support for older versions. Cherwell will use its best efforts to answer Customer's specific questions and provide support in accordance with Cherwell's service and support guidelines. Support does not include any third party products that are not part of the Licensed Software.   If Support is purchased from and provided directly by a Partner, as described in Section 7.7 below, then the terms and conditions of any agreement between Customer and Partner shall govern with regard to Support.

5.4   Professional Services. Where provided by and purchased from Cherwell, "Professional Services" may include training, implementation, installation, on-site assistance, customization, and configuration of the Licensed Software. The total "Professional Services" fee quoted on the Cherwell Order Confirmation Form, if any, is an estimate of the number of days required based on Cherwell's current understanding of Customer's stated implementation requirements.   A statement of work shall be mutually agreed upon prior to commencement of any Professional Services. Any professional or related services purchased from and provided directly by a Partner, as described in Section 7.7 below, shall be governed by the terms and conditions of any agreement between Customer and Partner.

6.   CONFIDENTIALITY

6.1   Definition. As used in this Agreement, "Confidential Information" means any information, whether oral or written, designated by a party as confidential or that reasonably should be understood to be confidential or proprietary in nature. Customer's Confidential Information shall include Customer data stored or processed with the Licensed Software.   Cherwell's Confidential Information shall include the Licensed Software. Confidential Information of each party shall include the terms of this Agreement (but not the fact of its existence), as well as each party's business and marketing plans, financial data, employee data, product plans and designs, and technical information. However, Confidential Information shall not include any information that (i) is or becomes generally known to the public other than by breach of this Agreement; (ii) was known to the receiving party prior to its disclosure; (iii) becomes known to the receiving party after proper disclosure from a third party not under an obligation of confidentiality; or (iv) was disclosed to the minimum extent necessary to comply with a lawful court order or government law or regulation, including the Texas Public Information Act (currently codified under Tex. Govt. Code Chapter 552), provided that in the case of (iv) the

disclosing party shall provide the other party with advance written notice thereof and reasonably cooperate with the other party to limit disclosure and obtain protective orders or other relief as appropriate.

6.2   Protection. Each party agrees to hold the other party's Confidential Information in strict confidence and to treat such other party's Confidential Information with at least the same degree of care employed with respect to its own Confidential Information (but in no event less than reasonable care). Neither party shall (i) use the other party's Confidential Information for its own account or in any manner not contemplated by this Agreement; nor (ii) disclose the other party's Confidential Information to a third party without the prior written consent of the other party. Both parties shall limit access of each other's Confidential Information to those of its employees, contractors and agents who have a need for such access and who are bound to confidentiality obligations substantially similar to those set forth in this Section. This Section shall survive termination or expiration of the Agreement (for any reason) for a period of three (3) years.

7.   MISCELLANEOUS

7.1   Severability. If any of the terms, or portions thereof, of this Agreement are invalid or unenforceable under any applicable statute or rule of law, the court shall reform the Agreement to include an enforceable term as close to the intent of the original term as possible; all other terms shall remain unchanged.

7.2   Entire Agreement. This Agreement constitutes the entire agreement between Customer and Cherwell relating to the subject matter hereof and supersedes all prior and contemporaneous agreements, representations, proposals and negotiations, whether written or oral. Any additions to, or modifications of, this Agreement shall be binding upon the parties only if in writing and executed by a duly authorized representative of Customer and Cherwell. TERMS AND CONDITIONS OF ANY CORRESPONDING PURCHASE ORDER OR OTHER DOCUMENT RELATING TO THE LICENSED SOFTWARE THAT ADD TO OR CONFLICT WITH THE TERMS CONTAINED IN THIS AGREEMENT SHALL BE DEEMED MATERIAL AND ARE REJECTED.

7.3   Waiver. The waiver or failure of either party to exercise in any respect any right provided for in this Agreement shall not be deemed a waiver of any further or future right under this Agreement.

7.4   RESERVED.

7.5   RESERVED.

7.6   Choice of Law. This Agreement is governed under the laws of the state of Texas, without regard to its conflicts of laws principles. This Agreement will not be governed by the United Nations Convention on Contracts for the International Sale of Goods, the application of which is expressly excluded.

7.7   Third Parties and Third Party Resellers. No person who is not a party to this Agreement has or shall have any right to enforce any term of this Agreement and no consent of any third party shall be required for any cancellation or variation of the Agreement. From time to time, Cherwell may authorize certain third parties, such as value-added resellers or solutions partners ("Partners"), to resell the Licensed Software and

Maintenance and Support Services. Customer acknowledges that as between Customer and Cherwell, Partners are not authorized to modify the terms and conditions of this Agreement nor the rights granted to Customer with regard to the Licensed Software. In certain jurisdictions or markets, Customer may purchase, from the Partner (rather than Cherwell), Support Services and Professional Services to be performed by the Partner. In such case, the terms of any agreement between Customer and Partner for such services shall govern, and Cherwell shall not be liable or otherwise responsible for Partner's performance or non-performance under such agreement. Maintenance, as described in this Agreement, shall in all cases be provided by Cherwell, subject to the terms of this Agreement.

7.8   RESERVED

Signature lines for the EUSA are located on the Cherwell Order Confirmation form to which the EUSA is incorporated by reference.

<u>EXHIBIT A</u>

Airport Security Requirements

PART 1 – GENERAL

SUMMARY

A.   Access to any security or emergency documents must be approved by the Security Manager. Due to the ever changing environment of Airport security, requirements may change at any time. SENSITIVE SECURITY INFORMATION must be protected at all times.

WARNING: This document contains Sensitive Security Information that is controlled under 49 CFR parts 15 and 1520. No part of this document may be disclosed to persons without a "need to know", as defined in 49 CFR parts 15 and 1520, except with the written permission of the Administrator of the TSA or the Secretary of Transportation. Unauthorized release may result in civil penalty or other action. For US government agencies public disclosure is governed by 5 U.S.C. 552 and CFR part 15 and 1520.

1.3   RESTRICTED AREAS ACCESS POLICIES
Escorted Access: For this project Individuals will submit to a fingerprint-based ten-year criminal history records check (CHRC) and Security Threat Assessment (STA). If the process confirms no disqualifying criminal offenses, the Department of Aviation (DOA) Security and ID Office will allow access, as approved by the Security Manager, to security areas and security documents. The Department of Aviation will provide escort services as part of this project as needed. Requests for access must be submitted in writing in advanced to the Security Manager so work can be scheduled accordingly.

Telecommunication / Electrical / Maintenance Room Access: The DOA Information Systems Division will approve access into DOA telecommunication rooms. The DOA Building Maintenance Division will approve access into electrical and/or maintenance rooms. A DOA employee will accompany and escort individuals needing access to these areas. Requests for escorts must be made at least three (3) working days in advance of the event through the Project Manager and/or at the Work Coordination Meetings.

The following procedures will be followed for approved parking:
The Vendor will contact Airport Communications (530-2242) to advise they are arriving at the terminal, or have arrived at their approved parking location. An Airport Security Supervisor or designee will be dispatched to meet at the designated parking location.
The security representative will inspect the vehicle and apply a distinctive sticker to the vehicle window to indicate that the vehicle has been inspected and authorized to be parked at that location.

Under no circumstances will the Vendor's vehicle operator leave the vehicle prior to security inspection.

1.4   SECURITY CLEARANCE PROCEDURES

Vendor should allow 7-10 days for completion of security screening processing. Please contact Security and ID at 530-6360 for business hours.

The following procedures will be followed to obtain security clearance:
Contract applicant will complete, sign the Personal Information Form, and present two forms of identification.

Contract applicant will read and sign the Criminal History Records Check/Disqualifying Criminal Offenses statement/form.

Vendor will submit to an FBI fingerprint-based criminal history records check and a TSA Security Threat Assessment (STA).

Non-U.S. citizen proposers will provide governmental proof of work authorization and an Aviation Department Documentation Verification Form reviewed and stamped by Immigration and Customs Enforcement personnel located on the ground level of the terminal building.

City of Austin - Aviation Department
Non-Disclosure Agreement

This Agreement is entered into this ___ day of _____ by and between _____ with offices at _____ (hereinafter "Recipient") and The City of Austin, by and through the Executive Director of the Department of Aviation, with offices at 3600 Presidential Boulevard, Austin, Texas 78719 (hereinafter "COA-DOA").

WHEREAS COA-DOA possesses certain ideas and information relating that is confidential and proprietary to COA-DOA (hereinafter "Confidential Information"); and

WHEREAS the Recipient is willing to receive disclosure of the Confidential Information pursuant to the terms of this Agreement for the purpose _____;

NOW THEREFORE, in consideration for the mutual undertakings of the COA-DOA and the Recipient under this Agreement, the parties agree as follows:

1. <u>Disclosure</u>. COA-DOA agrees to identify and disclose Confidential Information to the Recipient; the Recipient agrees to receive the Confidential Information.

2. <u>Confidentiality</u>.

   a. No Use. The Recipient agrees not to use the Confidential Information in any way, or to manufacture or test any product embodying Confidential Information, except for the purpose set forth above.
   b. No Disclosure. The Recipient agrees to use its best efforts to prevent and protect the Confidential Information, or any part thereof, from disclosure to any person other than the Recipient's employees having a need for disclosure in connection with the Recipient's authorized use of the Confidential Information.
   c. Protection of Secrecy. The Recipient agrees to take all steps reasonably necessary to protect the secrecy of the Confidential Information, and to prevent the Confidential Information from falling into the public domain or into the possession of unauthorized persons.

3. <u>Limits on Confidential Information</u>. Confidential Information shall not be deemed proprietary and the Recipient shall have no obligation with respect to such information where the information:
   a. was known to the Recipient's prior to receiving any of the Confidential Information from COA-DOA;
   b. has become publicly known through no wrongful act of the Recipient;
   c. was received by the Recipient without breach of this Agreement from a third party without restriction as to the use and disclosure of the information;
   d. was independently developed by the Recipient without use of the Confidential Information; or
   e. was ordered to be publicly released by the requirement of a government agency ("Order") provided that (i) Recipient shall immediately notify COA-DOA of such Order; and (ii) unless Recipient would be subject to sanctions from a court or other

governmental entity, Recipient shall not produce or disclose Confidential Information in response to the Order unless COA-DOA has: (a) requested protection from the government agency issuing the Order ("Protection") and such request has been denied, (b) consented in writing to the production or disclosure of the Confidential Information in response to the Order, or (c) takes no action to protect its interest in the Confidential Information within 10 business days after receipt of notice from Recipient of its obligation to disclose Confidential Information in response to the Order. Recipient shall cooperate with any efforts by COA-DOA to seek Protection and shall take all reasonable and lawful actions permitted under applicable law to avoid and/or minimize the extent of any disclosure of Confidential Information.

4. <u>Ownership of Confidential Information</u>. The Recipient agrees that all Confidential Information shall remain the property of COA-DOA, and that COA-DOA may use such Confidential Information for any purpose without obligation to the Recipient. Nothing contained herein shall be construed as granting or implying any transfer of rights to the Recipient in the Confidential Information, or any patents or other intellectual property protecting or relating to the Confidential Information.

5. <u>Term and Termination</u>. The obligations of this Agreement shall be continuing until the submission of the proposal at which point all data provided by the COA-DOA must be returned.

6. <u>Survival of Rights and Obligations</u>. This Agreement shall be binding upon, inure to the benefit of, and be enforceable by (a) COA-DOA, its successors, and assigns; and (b) the Recipient, its successors, and assigns.

7. CITY REPRESENTS THAT IT HAS THE RIGHT TO DISCLOSE CONFIDENTIAL INFORMATION, PROVIDED THAT ITS CONFIDENTIALITY IS PROTECTED BY RECIPIENT HEREUNDER. NO OTHER WARRANTIES ARE MADE. ALL CONFIDENTIAL INFORMATION DISCLOSED HEREUNDER IS PROVIDED "AS IS".

8. Recipient acknowledges that damages for improper disclosure of Confidential Information may be irreparable; therefore, COA-DOA is entitled to seek equitable relief, including injunction and preliminary injunction, in addition to all other remedies available to it.

9. This Agreement does not create an agency or partnership relationship. This Agreement will not be assignable or transferable by Recipient without the prior written consent of COA-DOA.

10. This Agreement may be executed in two or more identical counterparts, each of which shall be deemed to be an original and all of which taken together shall be deemed to constitute the agreement when a duly authorized representative of each party has signed the counterpart.

11. This Agreement constitutes the entire agreement between the Parties with respect to the subject matter hereof, and supersedes any prior oral or written agreements, and all contemporaneous oral communications pertaining to such subject matter. All additions or modifications to this Agreement must be made in writing and must be signed by both parties. Any failure to enforce a provision of this Agreement shall not constitute a waiver

thereof or any other provision.

12. This Agreement shall be governed by the laws of the State of Texas, without reference to conflict of laws principles. The exclusive venue for any dispute shall be in Travis County, Texas.

IN WITNESS WHEREOF, the parties have executed this agreement effective as of the date first written above.

RECIPIENT (Creative Enterprise Solutions, LLC dba BEYOND2-)

Signed: *Brian Flora*

Print Name: **Brian Flora**

Title: **Principal**

Date: **6 August, 2019**

CITY OF AUSTIN (COA-DOA)
DEPARTMENT OF AVIATION

Signed: _____

Print Name: Sai Purcell

Title: Procurement Supervisor

Date: 8/8/2019

BEYOND 20

Information Technology Service Management Software Solution
RFP 8100 PAX3147
Austin-Bergstrom International Airport

Thursday, January 17th, 2019 | 2:00 p.m.

PREPARED BY:

Yas Kusakawa
yas.kusakawa@beyond20.com
866-856-3117

60 E Rio Salado Parkway
Suite 900
Tempe, AZ 85281

Austin-Bergstrom
International Airport

Table of Contents

Cover Letter

Evaluation Team,

Beyond20 would like to thank the Austin-Bergstrom International Airport for the opportunity to be considered as your IT Service Management solution partner. We have endeavored to address the items in the solicitation comprehensively, but if there are areas in which more information would be helpful as you make your decision, please do not hesitate to ask.

As we understand it, the Airport is seeking a qualified vendor to support its initiative to replace its existing HEAT help desk system. The solution should support the Airport's transition into a service management organization and deliver training and software to further the Airport's ITSM goals.

The solution should include the following features:

- Incident Management/Service Request
- Problem Management
- Change Management

- Knowledge Management
- Self-Service Portal
- Dashboards and Reporting

Our offering comprises of a solution from Cherwell Software supported by Beyond20's unique industry experience working with local government and expertise in implementing Cherwell Service Management to meet different business needs. As a full-service business transformation firm, Beyond20 is positioned to offer a more complete and holistic solution than any software vendor, and we are free to recommend the ideal solution without bias.

It's probably best to start with an explanation of why Beyond20 is an ideal partner for the Airport:

Beyond20 is an Award-Winning Cherwell partner – Our experienced team excels at getting the most out of Cherwell, and our solutions built on the CSM Platform have been widely recognized. Beyond20's multi-pronged approach to information gathering creates a real-time understanding of the organization and informs the development of your specific deliverables.

Beyond20 has extensive, in-house, ITIL expertise – Not only do we implement Cherwell, we are an accredited ITIL training organization with a team of ITIL Experts that are recognized experts in the field – writers and speakers with extensive, real-world ITIL experience.

Beyond20's experience working with local governments – We know and understand the unique challenges you face, and we are positioned to help design a tailored solution that works for your management, your IT Department, and your customers.

Our proposed solutions consist of Cherwell Service Management:

Cherwell Service Management's abundance of unique capabilities (with respect to both functionality and ease of use) sets it apart from other ITSM solutions. Many of these unique capabilities align specifically with the requirements enumerated in the solicitation, as discussed in the following sections. Additional unique and noteworthy Cherwell capabilities include but are certainly not limited to the following:

cherwell

Flexible Deployment Model. Cherwell provides one of the most flexible deployment models of any ITSM tool. It can be deployed either as "On-Premise" or as "SaaS (Software-as-a-Service)" with no functional differences. Cherwell is an industry leader in ITSM SaaS delivery capabilities. Their hybrid 3.0 SaaS approach offers more flexibility and choices than any other service desk software provider on the market, and it is easy to switch between the models as your organization and its needs change. It can be deployed either as **"On-Premise"** or as **"SaaS (Software-as-a-Service)."**

All customizations and configurations are retained after upgrades. No matter how many times you upgrade to a new version, you'll never lose any of your configurations or customizations.

Codeless business application platform. This means that ANY business process whatsoever can be implemented and automated in Cherwell, all without writing code. Our customers use this feature to consolidate multiple solutions onto a single platform – think of Cherwell as a rapid development platform enabling the in-house development of business automation. This goes well beyond IT: *if you can draw it on a whiteboard, it can be automated in Cherwell.*

Fantastic dashboards and reporting capability. The reporting capability is superb. Even better: viewing reports and dashboards does not consume a license. This allows executives and stakeholders to have their own dashboards without extra cost. Some customers use this feature to generate "big screen" dashboards for display on large monitors in lobbies, call centers, NOCs – all at no extra cost.

Customer-friendly licensing model. All modules are included under a single license, so there's no need to go back to the vendor as your processes mature or you start using the software in a different way (e.g. more mobile devices). Concurrent licensing means you'll have to purchase fewer licenses for a given headcount, and many Cherwell features do not require a license at all.

We work with a lot of clients in local government; it's an area we like and believe in. In fact, some of our team members have extensive work history in local government. We're excited about this project and the opportunity to really make a difference at the Austin-Bergstrom International Airport.

At Beyond20 we love what we do, and we think it comes through in the quality of our work. We look forward to the opportunity to earn your business.

Regards,

Yas Kusakawa

Business Relationship Manager | Beyond20
Beyond20 is a DBE certified minority-owned, woman-owned small business.
Training | Consulting | Implementation
Email: yasuhiro.kusakawa@beyond20.com
Toll-free: (866) 856-3117

Tab 1) City of Austin Purchasing Office Documents

See following pages for:

- Signed Offer Sheet
- Section 0605 Local Business Presence Identification Form
- Section 0630 Exceptions
- Section 0800 Non-Discrimination and Non-Retaliation Certification
- Section 0815 Living Wages Contractor Certification
- Section 0835 Nonresident Bidder Provisions
- Section 0840 Service-Disabled Veteran Business Enterprise
- Section 0900 Subcontracting/Sub-consulting Utilization Form
- Signed Addendums

CITY OF AUSTIN, TEXAS
Purchasing Office
REQUEST FOR PROPOSAL (RFP)
OFFER SHEET

SOLICITATION NO: RFP 8100 PAX3147
DATE ISSUED: 11/12/2018

REQUISITION NO.: 8100 1801100035

COMMODITY CODE: 20811, 92045

FOR CONTRACTUAL AND TECHNICAL ISSUES CONTACT THE FOLLOWING AUTHORIZED CONTACT PERSON:

Sai Xoomsai Purcell

Procurement Specialist IV
Phone: (512) 974-3058
E-Mail: sai.xoomsai@austintexas.gov

Dan Dellemonache
Procurement Specialist III
Phone: (512) 974-2981
E-Mail: dan.dellemonache@austintexas.gov

COMMODITY/SERVICE DESCRIPTION: Information Technology Service Management Software Solution

PRE-PROPOSAL CONFERENCE TIME AND DATE: 11/27/2018, 2:30 pm, local time
LOCATION: 2716 Spirit of Texas Drive, Austin, TX 78717, The Oak Room
CONFERENCE CALL NO: 512-974-9300
CODE: 521387

PROPOSAL DUE PRIOR TO: 01/08/2019, 2:00 pm, local time

PROPOSAL OPENING TIME AND DATE: 01/08/2019, 3:00 pm, local time
LOCATION: MUNICIPAL BUILDING, 124 W 8th STREET RM 308, AUSTIN, TEXAS 78701

LIVE SOLICITATION OPENING ONLINE: For RFP's, only the names of respondents will be read aloud

For information on how to attend the Solicitation Closing online, please select this link:

http://www.austintexas.gov/department/bid-opening-webinars

When submitting a sealed Offer, use the proper address for the type of service desired, as shown below:

Address for US Mail (Only)	Address for FedEx, UPS, Hand Delivery or Courier Service
City of Austin	City of Austin, Municipal Building
Purchasing Office-Response Enclosed for Solicitation # RFP 8100 PAX3147	Purchasing Office-Response Enclosed for Solicitation # RFP 8100 PAX3147
P.O. Box 1088	124 W 8th Street, Rm 308
Austin, Texas 78767-8845	Austin, Texas 78701
	Reception Phone: (512) 974-2500

NOTE: Offers must be received and time stamped in the Purchasing Office prior to the Due Date and Time. It is the responsibility of the Offeror to ensure that their Offer arrives at the receptionist's desk in the Purchasing Office prior to the time and date indicated. Arrival at the City's mailroom, mail terminal, or post office box will not constitute the Offer arriving on time. See Section 0200 for additional solicitation instructions.

All Offers (including Compliance Plans) that are not submitted in a sealed envelope or container will not be considered.

SUBMIT 1 ORIGINAL AND 4 ELECTRONIC COPY (USB FLASH DRIVE) OF YOUR RESPONSE

SIGNATURE FOR SUBMITTAL REQUIRED ON PAGE 3 OF THIS DOCUMENT

This solicitation is comprised of the following required sections. Please ensure to carefully read each section including those incorporated by reference. By signing this document, you are agreeing to all the items contained herein and will be bound to all terms.

SECTION NO.	TITLE	PAGES
0100	STANDARD PURCHASE DEFINITIONS	*
0200 V2	STANDARD SOLICITATION INSTRUCTIONS, UPDATED JUNE 26, 2018	*
0300	STANDARD PURCHASE TERMS AND CONDITIONS	*
0400	SUPPLEMENTAL PURCHASE PROVISIONS	7
0401	SUPPLEMENTAL PURCHASE PROVISIONS – CLOUD COMPUTING REQUIREMENTS	9
0500	SCOPE OF WORK	10
0600	PROPOSAL PREPARATION INSTRUCTIONS & EVALUATION FACTORS	8
0601	PRICE PROPOSAL SHEET	4
0630	EXCEPTION FORM – Complete and return if applicable	1
0605	LOCAL BUSINESS PRESENCE IDENTIFICATION FORM – Complete and return	2
0800	NON-DISCRIMINATION AND NON-RETALIATION CERTIFICATION–Complete and return	2
0805	NON-SUSPENSION OR DEBARMENT CERTIFICATION	*
0810 V2	NON-COLLUSION, NON-CONFLICT OF INTEREST, AND ANTI-LOBBYING CERTIFICATION, UPDATED JUNE 26, 2018	*
0815	LIVING WAGES CONTRACTOR CERTIFICATION–Complete and return	1
0835	NONRESIDENT BIDDER PROVISIONS – Complete and return	1
0840	SERVICE-DISABLED VETERAN BUSINESS ENTERPRISE – Complete and return	1
0900	SUBCONTRACTING/SUB-CONSULTING UTILIZATION FORM – Complete & return	1
0905	SUBCONTRACTING/SUB-CONSULTING UTILIZATION PLAN – Complete and return if applicable	3
Exhibit A	Aviation Department Non-Disclosure Agreement	3
Attachment A	ITSM SERVICE MANAGEMENT SOFTWARE SOLUTION REQUIREMENTS – Complete and return	7 Tabs

* Documents are hereby incorporated into this Solicitation by reference, with the same force and effect as if they were incorporated in full text. The full text versions of the * Sections are available on the Internet at the following online address:

http://www.austintexas.gov/financeonline/vendor_connection/index.cfm#STANDARDBIDDOCUMENTS

If you do not have access to the Internet, you may obtain a copy of these Sections from the City of Austin Purchasing Office located in the Municipal Building, 124 West 8th Street, Room #308 Austin, Texas 78701; phone (512) 974-2500. Please have the Solicitation number available so that the staff can select the proper documents. These documents can be mailed, expressed mailed, or faxed to you.

The undersigned, by his/her signature, represents that he/she is submitting a binding offer and is authorized to bind the respondent to fully comply with the solicitation document contained herein. The Respondent, by submitting and signing below, acknowledges that he/she has received and read the entire document packet sections defined above including all documents incorporated by reference, and agrees to be bound by the terms therein.

Company Name: Creative Enterprise Solutions, L.L.C dba Beyond20

Company Address: 60 E Rio Salado Pkwy STE 900

City, State, Zip: Tempe, AZ 85281

Vendor Registration No.

Printed Name of Officer or Authorized Representative: Yasuhiro Kusakawa

Title: Business Relationship Manager

Signature of Officer or Authorized Representative:

Date: 1/14/2019

Email Address: yas.kusakawa@beyond20.com

Phone Number: 866-856-3117

* Proposal response must be submitted with this signed Offer sheet to be considered for award

Section 0605: Local Business Presence Identification

A firm (Offeror or Subcontractor) is considered to have a Local Business Presence if the firm is headquartered in the Austin Corporate City Limits, or has a branch office located in the Austin Corporate City Limits in operation for the last five (5) years, currently employs residents of the City of Austin, Texas, and will use employees that reside in the City of Austin, Texas, to support this Contract. The City defines headquarters as the administrative center where most of the important functions and full responsibility for managing and coordinating the business activities of the firm are located. The City defines branch office as a smaller, remotely located office that is separate from a firm's headquarters that offers the services requested and required under this solicitation.

OFFEROR MUST SUBMIT THE FOLLOWING INFORMATION FOR EACH LOCAL BUSINESS (INCLUDING THE OFFEROR, IF APPLICABLE) TO BE CONSIDERED FOR LOCAL PRESENCE.

NOTE: ALL FIRMS MUST BE IDENTIFIED ON THE MBE/WBE COMPLIANCE PLAN OR NO GOALS UTILIZATION PLAN (REFERENCE SECTION 0900).

USE ADDITIONAL PAGES AS NECESSARY

OFFEROR:

Name of Local Firm	Creative Enterprise Solutions, L.L.C. dba Beyond20	
Physical Address	60 E Rio Salado Pkwy STE 900 Tempe, AZ 85281	
Is your headquarters located in the Corporate City Limits? (circle one)	Yes	No
or		
Has your branch office been located in the Corporate City Limits for the last 5 years?	Yes	No
Will your business be providing additional economic development opportunities created by the contract award? (e.g., hiring, or employing residents of the City of Austin or increasing tax revenue?)	Yes	No

SUBCONTRACTOR(S):

Name of Local Firm	NOT APPLICABLE	
Physical Address		
Is your headquarters located in the Corporate City Limits? (circle one)	Yes	No
or		
Has your branch office been located in the Corporate City Limits for the last 5 years	Yes	No

Will your business be providing additional economic development opportunities created by the contract award? (e.g., hiring, or employing residents of the City of Austin or increasing tax revenue?)	Yes	No

SUBCONTRACTOR(S):

Name of Local Firm	NOT APPLICABLE	
Physical Address		
Is your headquarters located in the Corporate City Limits? (circle one)	Yes	No
or		
Has your branch office been located in the Corporate City Limits for the last 5 years	Yes	No
Will your business be providing additional economic development opportunities created by the contract award? (e.g., hiring, or employing residents of the City of Austin or increasing tax revenue?)	Yes	No

City of Austin, Texas

Equal Employment/Fair Housing Office

To: City of Austin, Texas,

I hereby certify that our firm complies with the Code of the City of Austin, Section 5-4-2 as reiterated below, and agrees:

(1)   Not to engage in any discriminatory employment practice defined in this chapter.

(2)   To take affirmative action to ensure that applicants are employed, and that employees are treated during employment, without discrimination being practiced against them as defined in this chapter, including affirmative action relative to employment, promotion, demotion or transfer, recruitment or recruitment advertising, layoff or termination, rate of pay or other forms of compensation, and selection for training or any other terms, conditions or privileges of employment.

(3)   To post in conspicuous places, available to employees and applicants for employment, notices to be provided by the Equal Employment/Fair Housing Office setting forth the provisions of this chapter.

(4)   To state in all solicitations or advertisements for employees placed by or on behalf of the Contractor, that all qualified applicants will receive consideration for employment without regard to race, creed, color, religion, national origin, sexual orientation, gender identity, disability, sex or age.

(5)   To obtain a written statement from any labor union or labor organization furnishing labor or service to Contractors in which said union or organization has agreed not to engage in any discriminatory employment practices as defined in this chapter and to take affirmative action to implement policies and provisions of this chapter.

(6)   To cooperate fully with City and the Equal Employment/Fair Housing Office in connection with any investigation or conciliation effort of the Equal Employment/Fair Housing Office to ensure that the purpose of the provisions against discriminatory employment practices are being carried out.

(7)   To require of all subcontractors having 15 or more employees who hold any subcontract providing for the expenditure of $2,000 or more in connection with any contract with the City subject to the terms of this chapter that they do not engage in any discriminatory employment practice as defined in this chapter

For the purposes of this Offer and any resulting Contract, Contractor adopts the provisions of the City's Minimum Standard Non-Discrimination and Non-Retaliation Policy set forth below.

City of Austin
Minimum Standard Non-Discrimination and Non-Retaliation in Employment Policy

As an Equal Employment Opportunity (EEO) employer, the Contractor will conduct its personnel activities in accordance with established federal, state and local EEO laws and regulations.

The Contractor will not discriminate against any applicant or employee based on race, creed, color, national origin, sex, age, religion, veteran status, gender identity, disability, or sexual orientation. This policy covers all aspects of employment, including hiring, placement, upgrading, transfer, demotion, recruitment, recruitment advertising, selection for training and apprenticeship, rates of pay or other forms of compensation, and layoff or termination.

The Contractor agrees to prohibit retaliation, discharge or otherwise discrimination against any employee or applicant for employment who has inquired about, discussed or disclosed their compensation.

Further, employees who experience discrimination, sexual harassment, or another form of harassment should immediately report it to their supervisor. If this is not a suitable avenue for addressing their compliant, employees are advised to contact another member of management or their human resources representative. No employee shall be discriminated against, harassed, intimidated, nor suffer any reprisal as a result of reporting a violation of this policy. Furthermore, any employee, supervisor, or manager who becomes aware of any such discrimination or harassment should immediately report it to executive management or the human resources office to ensure that such conduct does not continue.

Contractor agrees that to the extent of any inconsistency, omission, or conflict with its current non-discrimination and non-retaliation employment policy, the Contractor has expressly adopted the provisions of the City's Minimum Non-Discrimination Policy contained in Section 5-4-2 of the City Code and set forth above, as the Contractor's Non-Discrimination Policy or as an amendment to such Policy and such provisions are intended to not only supplement the Contractor's policy, but will also supersede the Contractor's policy to the extent of any conflict.

UPON CONTRACT AWARD, THE CONTRACTOR SHALL PROVIDE THE CITY A COPY OF THE CONTRACTOR'S NON-DISCRIMINATION AND NON-RETALIATION POLICIES ON COMPANY LETTERHEAD, WHICH CONFORMS IN FORM, SCOPE, AND CONTENT TO THE CITY'S MINIMUM NON-DISCRIMINATION AND NON-RETALIATION POLICIES, AS SET FORTH HEREIN, **OR** THIS NON-DISCRIMINATION AND NON-RETALIATION POLICY, WHICH HAS BEEN ADOPTED BY THE CONTRACTOR FOR ALL PURPOSES WILL BE CONSIDERED THE CONTRACTOR'S NON-DISCRIMINATION AND NON-RETALIATION POLICY WITHOUT THE REQUIREMENT OF A SEPARATE SUBMITTAL.

Sanctions:

Our firm understands that non-compliance with Chapter 5-4 and the City's Non-Retaliation Policy may result in sanctions, including termination of the contract and suspension or debarment from participation in future City contracts until deemed compliant with the requirements of Chapter 5-4 and the Non-Retaliation Policy.

Term:

The Contractor agrees that this Section 0800 Non-Discrimination and Non-Retaliation Certificate of the Contractor's separate conforming policy, which the Contractor has executed and filed with the City, will remain in force and effect for one year from the date of filling. The Contractor further agrees that, in consideration of the receipt of continued Contract payment, the Contractor's Non-Discrimination and Non-Retaliation Policy will automatically renew from year-to-year for the term of the underlying Contract.

Dated this __14th__ day of __January__, __2019__

CONTRACTOR	Beyond20
Authorized Signature	
Title	Business Relationship Manager

Section 0815: Living Wages Contractor Certification

Pursuant to the Living Wages provision (reference Section 0400, Supplemental Purchase Provisions) the Contractor is required to pay to all employees of the Prime Contractor and all tiers of subcontractors directly assigned to this City contract a minimum Living Wage equal to or greater than $15.00 per hour.

(1) The below listed individuals are all known employees of the Prime Contractor and its subcontractors who are directly assigned to this contract, and all are compensated at wage rates equal to or greater than $15.00 per hour:

Employee Name	Employer	Prime or Sub	Your Normal Rate	Employee Job Title
Lauren Foiles	Beyond20	Prime	$206.25/hour	Project Manager
Christian Greenleaf	Beyond20	Prime	$206.25/hour	Solutions Consultant
Larry Martin	Beyond20	Prime	$243.75/hour	Solutions Architecht

(2) All future employees of both the Prime Contractor and all tiers of subcontractors directly assigned to this Contract will be paid a minimum Living Wage equal to or greater than $15.00 per hour.

(3) Our firm will not retaliate against any employee of either the Prime Contractor or any tier of subcontractors claiming non-compliance with the Living Wage provision.

A Prime Contractor or subcontractor that violates this Living Wage provision shall pay each of its affected employees the amount of the deficiency for each day the violation continues. Willful or repeated violations of the provision by either the Prime Contractor or any tier of subcontractor, or fraudulent statements made on this certification, may result in termination of this Contract for Cause, subject the violating firm to possible suspension or debarment, or result in legal action.

I hereby certify that all the listed employees of both the Prime Contractor and all tiers of subcontractors who are directly assigned to this contract are paid a minimum Living Wage equal to or greater than $15.00 per hour.

Contractor's Name:
Beyond20

Signature of Officer or Authorized Representative:

Date: 1/14/2019

Printed Name: Yasuhiro Kusakawa

Title   Business Relationship Manager

Section 0835: Non-Resident Bidder Provisions

Company Name ___Beyond20___

A. Bidder must answer the following questions in accordance with Vernon's Texas Statues and Codes Annotated Government Code 2252.002, as amended:

Is the Bidder that is making and submitting this Bid a "Resident Bidder" or a "non-resident Bidder"?

Answer: ___Non-Resident___

    (1) Texas Resident Bidder- A Bidder whose principle place of business is in Texas and includes a Contractor whose ultimate parent company or majority owner has its principal place of business in Texas.

    (2) Nonresident Bidder- A Bidder who is not a Texas Resident Bidder.

B. If the Bidder id a "Nonresident Bidder" does the state, in which the Nonresident Bidder's principal place of business is located, have a law requiring a Nonresident Bidder of that state to bid a certain amount or percentage under the Bid of a Resident Bidder of that state in order for the nonresident Bidder of that state to be awarded a Contract on such bid in said state?

Answer: ___No___   Which State: ___AZ___

C. If the answer to Question B is "yes", then what amount or percentage must a Texas Resident Bidder bid under the bid price of a Resident Bidder of that state in order to be awarded a Contract on such bid in said state?

Answer: _____

Offeror Name
Beyond20

Additional Solicitation Instructions.

1. ☒ By checking this box, Offeror states they are NOT a certified Service-Disabled Veteran Business Enterprise seeking to claim preference points under the City of Austin's SDVBE Program.

2. Offerors seeking to claim the Service-Disabled Veteran Business Enterprise (SDVBE) preference shall be certified **under one of the two following scenarios**. Offerors shall check one of the following boxes, input the data in the applicable table below and include this completed form in their Proposal.

   ☐ **HUB/SV**. Offeror is certified as a Service-Disabled Veteran (SV) Historically Underutilized Business (HUB) by the Texas State Comptroller of Public Accounts.

Texas State HUB/SV Certification	
13-Digit Vendor ID (VID)	
HUB/SV Issue Date	
HUB/SV Expiration Date	

   ☐ **HUB/OTHER + Federal SDVOSB**. Offeror is certified by the Texas State Comptroller of Public Accounts as a Historically Underutilized Business in a HUB Eligibility Category other than Service-Disabled Veteran (SV) AND is verified by the US Veterans Administration as a Service-Disabled Veteran-Owned Small Business (SDVOSB). **Texas HUB Eligibility Categories:** HUB/BL (Black), HUB/AS (Asian), HUB/HI (Hispanic), HUB/AI (Native American), or HUB/WO (Women Owned).

Texas State HUB/OTHER Certification			Federal SDVOSB Verification	
13-Digit Vendor ID (VID)			9-Digit DUNS	
HUB Eligibility Category			SDVOSB Issue Date	
HUB Issue Date			SDVOSB Expiration Date	
HUB Expiration Date				

3. <u>Offeror Identity</u>. The Offeror submitting the Proposal shall be the same entity that is certified by the Texas State Comptroller of Public Accounts, AND if applicable as verified by the US Veterans Administration.

4. <u>Certification Status</u>. Offeror's certification(s) must be active on or before the Solicitation's due date for Proposals and shall not expire prior to the award and execution of any resulting contract.

5. <u>Confirmation of Certification(s)</u>. Upon receipt of this completed form, the City will confirm the Offeror's certification(s): State: https://mycpa.cpa.state.tx.us/tpasscmblsearch. Federal: https://www.vip.vetbiz.gov/ The City will direct any questions concerning an Offeror's State or Federal certification status to the Offeror's contact person as designated on the Offer Form of their Proposal.

6. <u>Misrepresentation</u>. If the City determines that the Offeror requesting this preference is not certified by the State or Federal government if applicable, the Offeror will not receive the preference points. If the City determines that this misrepresentation was intentional, the City may also find the Offeror not responsible and may report the Offeror to the Texas State Comptroller of Public Accounts or if applicable to the US Veterans Administration. If the misrepresentation is discovered after contract award, the City reserves the right to void the contract.

Section 0900: SUBCONTRACTING/SUB-CONSULTING UTILIZATION FORM

MINORITY- AND WOMEN-OWNED BUSINESS ENTERPRISE (MBE/WBE)
PROCUREMENT PROGRAM
Subcontracting/Sub-Consulting ("Subcontractor") Utilization Form

SOLICITATION NUMBER: RFP 8100 PAX3147

SOLICITATION TITLE: INFORMATION TECHNOLOGY SERVICE MANAGEMENT SOFTWARE SOLUTION

In accordance with the City of Austin's Minority and Women-Owned Business Enterprises (M/WBE) Procurement Program (Program), Chapters 2-9A/B/C/D of the City Code and M/WBE Program Rules, this Solicitation was reviewed by the Small and Minority Business Resources Department (SMBR) to determine if M/WBE Subcontractor/Sub-Consultant ("Subcontractor") Goals could be applied. Due to insufficient subcontracting/subconsultant opportunities and/or insufficient availability of M/WBE certified firms, SMBR has assigned no subcontracting goals for this Solicitation. However, Offerors who choose to use Subcontractors must comply with the City's M/WBE Procurement Program as described below. Additionally, if the Contractor seeks to add Subcontractors after the Contract is awarded, the Program requirements shall apply to any Contract(s) resulting from this Solicitation.

Instructions:
a.) Offerors who do not intend to use Subcontractors shall check the "NO" box and follow the corresponding instructions.
b.) Offerors who intend to use Subcontractors shall check the applicable "YES" box and follow the instructions. **Offers that do not include the following required documents shall be deemed non-compliant or nonresponsive as applicable, and the Offeror's submission may not be considered for award.**

[X] **NO, I DO NOT intend to use Subcontractors/Sub-consultants.**

> **Instructions:** Offerors that do not intend to use Subcontractors shall complete and sign this form below (Subcontracting/Sub-Consulting ("Subcontractor") Utilization Form) and include it with their sealed Offer.

[ ] **YES, I DO intend to use Subcontractors /Sub-consultants.**

> **Instructions:** Offerors that do intend to use Subcontractors shall complete and sign this form below (Subcontracting/Sub-Consulting ("Subcontractor") Utilization Form), and follow the additional Instructions in the (Subcontracting/Sub-Consulting ("Subcontractor") Utilization Plan). Contact SMBR if there are any questions about submitting these forms.

Offeror Information	
Company Name	Creative Enterprise Solutions, LLC dba Beyond20
City Vendor ID Code	
Physical Address	60 E. Rio Salado Pkwy Ste 900
City, State Zip	Tempe AZ 85281
Phone Number	886-856-3117
Email Address	yas.kusakawa@beyond20.com
Is the Offeror City of Austin M/WBE certified?	[ ] NO [X] YES Indicate one: [X] MBE [X] WBE [ ] MBE/WBE Joint Venture

Offeror Certification: I understand that even though SMBR did not assign subcontract goals to this Solicitation, I will comply with the City's M/WBE Procurement Program if I intend to include Subcontractors in my Offer. I further agree that this completed **Subcontracting/Sub-Consulting Utilization Form,** and if applicable my completed **Subcontracting/Sub-Consulting Utilization Plan,** shall become a part of any Contract I may be awarded as the result of this Solicitation. Further, if I am awarded a Contract and I am not using Subcontractor(s) but later intend to add Subcontractor(s), before the Subcontractor(s) is hired or begins work, I will comply with the City's M/WBE Procurement Program and submit the **Request For Change** form to add any Subcontractor(s) to the Project Manager or the Contract Manager for prior authorization by the City and perform Good Faith Efforts (GFE), if applicable. I understand that, if a Subcontractor is not listed in my **Subcontracting/Sub-Consulting Utilization Plan,** it is a violation of the City's M/WBE Procurement Program for me to hire the Subcontractor or allow the Subcontractor to begin work, unless I first obtain City approval of my **Request for Change** form. I understand that, if a Subcontractor is not listed in my **Subcontracting/Sub-Consulting Utilization Plan,** it is a violation of the City's M/WBE Procurement Program for me to hire the Subcontractor or allow the Subcontractor to begin work, unless I first obtain City approval of my **Request for Change** form.

Yasuhiro Kusakawa	_(signature)_	1/14/2019
Name and Title of Authorized Representative (Print or Type)	Signature/Date	

| Solicitation: RFP 8100 PAX3147 | Addendum No: 1 | Date of Addendum: 11/29/2018 |

This addendum is to incorporate the following changes to the above referenced solicitation:

1. **Correction:** Section 0400, Supplemental Purchase Provisions, item 1.Explanations of Clarifications has been corrected as follow:

   All requests for explanations or clarifications must be submitted in writing to the Purchasing Office by email to Sai.Xoomsai@austintexas.gov or Daniel.Dellemonache@austintexas.gov by end of day 12/12/2017 12/12/2018.

2. ALL OTHER TERMS AND CONDITIONS REMAIN THE SAME.

11/29/2018

APPROVED BY: _____

Sai Purcell, Procurement Specialist IV   Date
Purchasing Office, 512-974-3058

ACKNOWLEDGED BY:

Yasuhiro Kusakawa   1/14/2019
Name   Authorized Signature   Date

RETURN ONE COPY OF THIS ADDENDUM TO THE PURCHASING OFFICE, CITY OF AUSTIN, WITH YOUR RESPONSE OR PRIOR TO THE SOLICIATION CLOSING DATE. FAILURE TO DO SO MAY CONSTITUTE GROUNDS FOR REJECTION.

Revised 12/13/2015

ADDENDUM
PURCHASING OFFICE
CITY OF AUSTIN, TEXAS

Solicitation: RFP 8100 PAX3147	Addendum No: 2	Date of Addendum: 12/04/2018

This addendum is to incorporate the following changes to the above referenced solicitation:

1. Q) Are City's Terms and Conditions negotiable?
    A) See below from Section 0600, Proposal Preparation Instructions and Evaluation Factors, Tab 1.C, Section 0630 Exceptions.

    Section 0630 Exceptions: Proposer shall clearly indicate each exception taken, provide alternative language, and justify the alternative language. The Proposer that is awarded the contract will be required to sign the contract with the provisions accepted; any exceptions may be negotiated or may result in the City deeming the offer non-responsive. Failure to accept or provide the exception information under **Purchasing Exceptions Form** may result in the City deeming the offer non-responsive. The City reserves the right to reject a Proposal containing exceptions, additions, qualifications, or conditions not called for in the Solicitation

2. Q) Section 0601, Price Proposal Sheet request pricing for 20 hours of onsite training per year. What type of training would the City like to be delivered in the 20 hours/year of onsite training?
    A) On site software and administration training for staff, i.e. new employee training, new features, set up of new features, configuration, new workflow development, etc.

3. Q) How important is it for the project management tool to live on the same platform as the ITSM tool with no additional cost added to access the tool or is the City looking to purchase an additional software platform to help with the City project management needs? When does the City envision incorporating a project management tool?
    A) A project management tool is out of scope for this project. Any integration between project management tools and IT Service Management tools is not under consideration at present.

4. Q) Has the City engaged any other venders prior to this RFP process? If yes, who are those vendors and what actions have been taken with those companies?
    A) No. The City has not engaged with any other venders prior to the RFP process.

5. Q) It was stated during the conference that the deadline to submit questions is December 12th, when can vendor expect a response to the questions?
    A) The estimated Addendum to the questions is expected by December 19, 2018

6. **Correction**: Dan Dellemonache email address:
    Daniel.Dellemonache@austintexas.gov

7.   ALL OTHER TERMS AND CONDITIONS REMAIN THE SAME.

APPROVED BY: _____   12/04/2018

            Sai Purcell, Procurement Specialist IV   Date
            Purchasing Office, 512-974-3058

ACKNOWLEDGED BY:

Yasuhiro Kusakawa _____   _____   1/14/2019
Name   Authorized Signature   Date

RETURN ONE COPY OF THIS ADDENDUM TO THE PURCHASING OFFICE, CITY OF AUSTIN, WITH YOUR RESPONSE OR PRIOR TO THE SOLICIATION CLOSING DATE. FAILURE TO DO SO MAY CONSTITUTE GROUNDS FOR REJECTION.

Solicitation: RFP 8100 PAX3147 **Addendum No: 3** **Date of Addendum: 12/17/2018**

This addendum is to incorporate the following changes to the above referenced solicitation:

1. Q)   How large is the Airport IT department?
   A)   57 including on site contractors

2. Q)   How many people work on the help desk?
   A)   12

3. Q)   What tool(s) (if any) aside from HEAT are being used to fulfill the functionalities being requested?
   A)   Excel, Word, KanBoard

4. Q)   Is importing data from the current system within the scope of this project? If so, how many records will need to be imported?
   A)   No service tickets will be imported. It's possible some of the client contact information may be imported.

5. Q)   Is there a prevailing event/initiative/etc. that triggered the creation and release of this solicitation?
   A)   No.

6. Q)   Does the Airport current have processes for the following ITSM?
   a.   Incident Management
   b.   Request Fulfillment
   c.   Problem Management
   d.   Change Management
   e.   Knowledge Management
   A)   The Airport currently have processes for Incident management, Request Fulfillment, Problem management, Change Management, but no process for Knowledge Management.

7. Q)   If there is a particular process that the Airport currently does not have established/documented, is the design of that process part of the scope of this project?
   A)   No. This work will be done by the Airport's On-Call contractor

8. Q)   Does the Airport currently have a well-defined Service Catalog?
   A)   Yes

9. Q)   Does the Airport currently have well-defined Service Level Agreements with its customers?
   A)   Some but not all.

10. Q)   Will there be multiple business units using this for processing tickets? If so, will these need to be broken out? Will they need separate service catalogs? Will they need separate portals?
    A)   No.

11. Q) Could the Airport provide a use case or user story that is representative of each of the Maximo integration desired, a use case or user story that is representative of each of the SCCM integration desired, a use case or user story that is representative of each of the Office365 integration desired, case or user story that is representative of each of the Cisco IP integration desired?

A) The Airport will utilize the stated expertise of the selected vendor, in conjunction with the Airport's On-Call contractor, to establish necessary use cases/stories for each of the expected software/tool integrations within the scope of the project. The Airport seeks a vendor experienced in successfully implementing an ITSM solution. The Airport will request the assistance of the selected vendor to more fully develop relevant and Airport-specific use cases/stories during the project.

12. Q) What tools, if any, would the Airport like the tool to integrate with? Could you please provide use cases for each?

A) Please refer to question 11

13. Q) Has a budget for this project been determined? If so, what is the budget for this project?

A) No budget has yet been set.

14. ALL OTHER TERMS AND CONDITIONS REMAIN THE SAME.

12/17/2018

APPROVED BY: _____

Sai Purcell, Procurement Specialist IV   Date
Purchasing Office, 512-974-3058

ACKNOWLEDGED BY:

Yasuhiro Kusakawa   1/14/2019
Name   Authorized Signature   Date

RETURN ONE COPY OF THIS ADDENDUM TO THE PURCHASING OFFICE, CITY OF AUSTIN, WITH YOUR RESPONSE OR PRIOR TO THE SOLICIATION CLOSING DATE. FAILURE TO DO SO MAY CONSTITUTE GROUNDS FOR REJECTION.

Solicitation: RFP 8100 PAX3147   **Addendum No: 4**   **Date of Addendum: 12/26/2018**

This addendum is to incorporate the following changes to the above referenced solicitation:

1. Q)   What is an average number of Incident, problem & change tickets per month?
    A)   The current ticketing system does not break out requests into these categories.

2. Q)   What is an average number of service requests per month?
    A)   The current ticketing system does not reflect the actual number of requests fulfilled as we do a lot of ad hoc work.

3. Q)   In the current ITSM environment, how many resolvers (both internal and 3rd party) are there today? Does the City expect this number to change?
    A)   The City currently service approximately 300-400 customers. The City does not track vendors in the current system.

4. Q)   How many Customer IDs vs Vendor IDs are there today? Does the City expect this number to change?
    A)   The City currently service approximately 300-400 customers. We do not track vendors in the current system.

5. Q)   Does the City currently have CMDB in scope today? If yes please describe its breadth and depth of services. Such as what layers are covered within Infrastructure components, business applications? Services? Servers etc...?
    A)   No. The City does not currently have CMDB in scope.

6. Q)   What is the number of configuration items?
    A)   This will be determined within the implementation project

7. Q)   What discovery tool is being used today, please provide the approximate number of nodes in your environment?
    A)   Microsoft SCCM

8. Q)   How are assets being managed by the IPC/ticketing tool and is your asset management tool it integrated with IPC/ticketing tool?
    A)   Assets are managed manually using spreadsheets. There is no integration.

9. Q)   Does the City IPC/ticketing tool get any auto generated tickets from HW/application monitoring tools? If so, which tools are used and please specify how many tickets are generated from each source.
    A)   No. The City IPC/ticketing tool does not get any auto generated tickets from HW/application monitoring tools.

10. Q) Please describe the City current reporting and the expectations for the future reporting environment. (example:-manual today, automated in the future; no tool / process aligned today, want to be tool / process aligned in the future, etc.)
    A) Very little reporting is available today. Would like to track KPIs and processes. Process aligned automated reporting in addition to adhoc and custom.

11. Q) Is the City reporting tool integrated to your IPC/ticketing tool?
    A) No

12. Q) Please describe if there are any data privacy concerns or implications of moving data across borders.
    A) No data be stored outside of the USA. There is security sensitive data that will be tracked in the system.

13. Q) Are there any bridges from your IPC tool to third party vendors?
    A) None

14. Q) What data or tools are integrated with your current IPC tool?
    A) None

15. Q) If there are vendors, are any tickets transferred either to (or) from these vendors via any bridge to their ticketing system? If so, please enumerate and describe.
    A) No. There are no vendors, tickets transferred either to (or) from these vendors via any bridge to their ticketing system

16. Q) What tools are currently used today by Client and suppliers today for Request Fulfillment?
    A) Email, SharePoint, excel

17. Q) To what extent is Request Fulfillment automated? How many service request types can be made? What is the volume of service requests?
    A) No automation

18. Q) Please provide number of Catalog Items broken down by complexity.
    A) The Service Catalog is currently being updated. These updates will continue through the ITSM Software Solution implementation project. Simple – NA, Medium – NA, Complex – NA.

19. Q) Does customer have SPI (sensitive personal information) data that will be entered in system?
    A) No.

20. Q) Does customer have any ITAR or any other regulatory requirements?
    A) No

21. Q) What are the onboarding requirements to work for this client?
    A) Review City of Austin, Texas Procurement Process and Requirements.

22. Q) Is there any delivery Location/resource restrictions for the implementation and ongoing support of ITSM tool?
    A) No.

23. Q) Is there a need for data segregation?
    A) No

24. ALL OTHER TERMS AND CONDITIONS REMAIN THE SAME.

12/26/2018

APPROVED BY: _____

Sai Purcell, Procurement Specialist IV   Date
Purchasing Office, 512-974-3058

ACKNOWLEDGED BY:

_Yasuhiro Kusakawa_____   _____   _1/14/2019_____
Name   Authorized Signature   Date

RETURN ONE COPY OF THIS ADDENDUM TO THE PURCHASING OFFICE, CITY OF AUSTIN, WITH YOUR RESPONSE OR PRIOR TO THE SOLICIATION CLOSING DATE. FAILURE TO DO SO MAY CONSTITUTE GROUNDS FOR REJECTION.

Solicitation: RFP 8100 PAX3147	Addendum No: 5	Date of Addendum: 12/27/2018

This addendum is to incorporate the following changes to the above referenced solicitation:

PROPOSAL DUE PRIOR TO: has been extended to 01/17/2019, 2:00 pm local time.

PROPOSAL OPENING TIME AND DATE: has been extended to 01/172019, 3:00 pm local time

PROPOSAL DUE PRIOR TO: 01/08/2019, **01/17/2019**, 2:00 pm, local time

PROPOSAL OPENING TIME AND DATE: 01/08/2019, **01/17/2019**, 3:00 pm, local time

1. ALL OTHER TERMS AND CONDITIONS REMAIN THE SAME.

APPROVED BY: _____

12/27/2018

Sai Purcell, Procurement Specialist IV
Purchasing Office, 512-974-3058

Date

ACKNOWLEDGED BY:

Yasuhiro Kusakawa
Name

Authorized Signature

1/14/2019
Date

RETURN ONE COPY OF THIS ADDENDUM TO THE PURCHASING OFFICE, CITY OF AUSTIN, WITH YOUR RESPONSE OR PRIOR TO THE SOLICIATION CLOSING DATE. FAILURE TO DO SO MAY CONSTITUTE GROUNDS FOR REJECTION.

Revised 12/13/2015

Cherwell Support Guidelines

Revision 3.0

September 1, 2017

Cherwell Software

www.cherwell.com

Contents

Scope of Support

Cherwell Support is designed to assist customers with specific product issues resulting from the normal use of the Cherwell Service Management software on supported platforms, and to provide resolutions/answers to those issues or questions. Cherwell is dedicated to partnering with customers to answer questions and resolve issues. Customers are expected to properly install, implement and use the software and comply with reasonable troubleshooting tasks as recommended by the Cherwell Support team.

Cherwell Support's primary responsibilities are:

- Troubleshooting issues related to the Cherwell Service Management software when unexpected results occur
- Reproducing product defects and providing assistance in alternative solutions or workarounds to help maintain stability until a defect is addressed/corrected
- Assisting with software maintenance updates and upgrades that offer solution fixes and minor or major product releases

Cherwell API Support:

- Cherwell will support the Cherwell Rest API pursuant to connectivity and only in accordance with the use of the Swagger Interface. Code samples can be found on the Help Site and Cherwell samples are from the Swagger-Code-Gen-Utility
- Cherwell will support the Cherwell SOAP API pursuant to connectivity and in accordance with the Cherwell Service Website
- Cherwell Support will not provide code samples nor review code
- Cherwell Support will assist in identifying any bug, enhancement or request for general documentation or procedures
- Cherwell does not support using the trebuchet.net API

Cherwell's support analysts are trained to support the licensed software and may not possess the qualifications to support Incidents outside the scope of Cherwell's licensed software (i.e., third-party integrations, environmental issues, etc.).

*Reference to Cherwell Software Management includes Cherwell Asset Management (CAM) and all supported versions of Express Metrix unless otherwise stated

Beyond the Scope of Maintenance and Support

Cherwell Support will assist in platform matters as they relate to the Cherwell System. Cherwell Support will not support customized business processes or design elements outside of the scope of platform. Cherwell support is not responsible for service issues arising from a need for training, implementation services, and customization services. Customers may be referred to the Cherwell Professional Services Organization where arrangements for appropriate services can be made.

Professional Service Requests include:

- **Education/Training**: Learning Services are provided through Cherwell's Professional Services Organization. A support analyst can help determine if consulting or training is required and will help you develop the best course of action to address your needs.
- **System Setup:** Requests that relate to a new implementation, setup of business processes, configuration, or the installation of new products.
- **Operating System/Hardware:** Requests related to hardware configuration, database administration, or operating-system modifications (unless hosted in Cherwell Cloud).
- **Fine-tuning Application Performance:** Analyzing, testing, and improving overall performance of Cherwell Service Management (unless hosted in Cherwell Cloud).
- **Customizing/Configuring Business Objects:** Support provides assistance with Cherwell's standard "out-of-the-box" solution set and custom implementation provided by Cherwell Professional Services and Certified Cherwell Partners. Incidents that relate to non-standard versions of the software are considered service requests and will be referred to Professional Services.
- **Developing Reports**: Cherwell Software Professional Report Writing Services specializes in the creation of reports and themes. Report writers are ITIL® Foundation certified and have a special certification from Cherwell Software in Report Writing.
- **Troubleshooting customer-developed Reports**: Cherwell Software Professional Reporting Writing Services can assist with troubleshooting issues that may arise in customer-developed reports by analyzing the report design to help determine the root cause of the issue.

Hours of Operation

Cherwell Support is available 24 hours a day, 365 days a Year.

Contacting Support

Support for the Cherwell Service Management software is available through a variety of contact methods which include Cherwell Self-Service, Telephone Support, E-mail Support, Remote Access Support, Cherwell Scheduled After-Hours Support, and Cherwell On-call/After-hours Support. We encourage customers to log Incidents through Cherwell Self-Service, the most efficient method which allows analysts to quickly begin the analysis and research required to resolve the issue.

- **Cherwell Self-Service**: A wide range of options for Cherwell Self-Service are available at

  www.cherwellsupport.com:

  - Product Documentation
  - Access to Cherwell Knowledge
  - Ability to view and update Incidents
  - Access to product information
  - Access to download the latest version of the product
  - Your User Id and password are included in your welcome letter; contact Support at

    support@cherwell.com if you have misplaced the information.

- **Telephone Support**: Call 719.386.7000 or +44 (0)1793 544899 (EMEA)

  - Support is available 24 hours a day, 365 days a year

- **E-mail Support**: Send e-mail to **support@cherwell.com**
  - For Cherwell Asset Management (previously known as Express Metrix) please use
    camsupport@cherwell.com

  Support is available 24 hours a day, 365 days a year

- **Remote Access Support**: With advance permission, Cherwell Support analysts may remotely access systems associated with Cherwell Service Management to help analyze and resolve issues with the licensed software.

Cherwell Self-Service, telephone, and e-mail support are available during regular support hours for supported versions of the licensed software, and only to customers with a current Maintenance and Support agreement or current with their subscription licenses. Cherwell Support does require that a customer upgrade to the current version to resolve a known problem or technical issue which likewise requires that a customer be current on Maintenance and Support or current with their subscription licenses. For more information, related to supported versions, please refer to Cherwell's Version Support Policy (see below). Best efforts will be made to provide a workaround for a known issue; however, Cherwell Support does not guarantee resolution to all software issues requiring changes to the software.

Cherwell Support inquiries are classified as Incidents. An Incident is a single, reproducible issue, symptom, or error inherent in the licensed software. Cherwell Support may determine that an Incident is in fact related to how the licensed software was implemented and/or is being used and indicates that the customer requires additional training or Professional Services. Cherwell Support will work with you to determine the best plan of action for Professional Services or Learning Services.

Customer Response

Please note that once a ticket is logged with Support and should we require additional information or a response from the customer with regards to that ticket, we will attempt to reach the customer 3 times before we will resolve the ticket. Cherwell Support will wait a period of 3 business days following the first request for response, indicating that the ticket will be placed on hold until we receive the information requested, if no response is received we will issue a further request, if after 3 more business days still no response is received the ticket will be set to "Resolved", you will then have 3 business days to re-open the incident by clicking the "Click to Reopen incident" hyperlink in the email you will receive as part of this process, before the incident will automatically go into "closed" state. Should contact be made after this point a new ticket will be logged. Tickets can be placed on hold at the customer request to cover long periods of accepted inactivity/communication.

Priority and Response Time Definitions

The following chart serves as a guide to understand how Cherwell Support assigns each Incident a Priority, as well as the Initial Response Time you can expect. An Incident is an unplanned interruption or reduction in quality of service. Please note that "Response Time" does not necessarily mean the amount of time it takes to resolve or close an issue; it does, however, reflect how much time it takes for Cherwell to acknowledge and provide an initial response to the issue on best effort.

Incident Response time expectations

Priority	Severity Level	Description	Target Response Time
1	Critical	The software is inaccessible or non-operational	2 hours
2	High	Performance of the software is severely degraded, or is negatively impacting business operations.	4 hours
3	Normal	There is an aspect of the way the software has been designed that is interfering with work.	1 day
4	Low	Requests that do not impact work, questions or documentation issues	2 days

Note: P1 or P2, critical issues should be reported via phone.

Requests for System Upgrades & Refreshes

Please note that System Upgrade and System Refresh requests will be dealt with as Priority 4 tickets with the associated response times as defined above. Cherwell Support require a minimum notice of 3 business days to carry out upgrades and refreshes.

All Test and Development System Refreshes or Upgrades will be scheduled between 8 am and 5 pm Mountain time or 9 am and 5.30 pm GMT (dependent on location of the hosted service).

Support of mApps

Cherwell Software's support obligation does not include providing technical assistance and resolving issues specifically related to the implementation of mApp technologies provided by third-parties which are specific to that mApp. Cherwell may provide troubleshooting to isolate the cause of any issues related to 3rd party mApp solutions. However, Cherwell will not make design recommendations or may not be able to fully remediate issues related to any customized configuration specific to a 3rd party mApp.

Once the 3rd party mApp has been implemented by the customer and is fully functional, Cherwell will provide support to analyze any issues related to the mApp but may need to refer to the original provider for assistance and further remediation.

Escalation of Incidents

An Incident may be escalated by you, Client Services or Support. If it is deemed that an Incident requires escalation, we will gather the necessary resources which may include Client Services, development, our Professional Services Organization, partners, and other resources as appropriate. You must also be prepared to make appropriate resources available to work with Cherwell.

Expectations

Your cooperation and effort are necessary to provide you with the quality of service you desire—it is only by working together that we can ensure our customers receive the most value from Cherwell Support.

NOTE: *If at any time during the resolution of an Incident a customer is unable to meet designated commitments or requirements, support may be suspended on the Incident until requirements can be met and a scheduled course of action arranged.*

Supported Platforms

For information detailing currently supported platforms, server and client requirements, client operating systems, and web application server requirements, please refer to related documentation provided on the Customer Support site.

Version Support Policy

Cherwell will provide support for the most current version of the Licensed Software and one prior version, including interim releases between the two versions; for example, upon release of version 9.x Cherwell will support version 9.x.x and 8.x.x. Support is provided in accordance with the provisions of the customers End-User License Agreement.

Cherwell Asset Management Updates & Downloads

Monthly CSID Updates (Cherwell Software Identification Database)

The CSID (previously Express Software Identification Database (ESID)®) is a comprehensive catalog of commercial and free PC software applications. Known throughout the industry for its accuracy and comprehensiveness, the CSID enables CAM/Express Software Manager products to identify the wide range of software installed and used across your network. Updated monthly, the ESID gives you the most up-to-date application recognition capabilities possible so you don't fall behind on your licensing.

Access to Special File Downloads

Maintained customers have access to downloads that are designed to increase product performance and decrease administration overhead. A WMI viewer, various utilities and product patches are all included in this category.

Best Practice Recommendations

System Administration

To obtain optimal results, Cherwell recommends two internal system administrators to manage and protect the integrity of the system and the company's data including:

- Documented system-management procedures
- Regular system backups and verifications
- Change management process to help track and manage changes to the system including the operating system, application environments, and database.
- Please note that if you are hosting Cherwell in the Cherwell Cloud, certain of these administrative functions will be conducted by the Cherwell DBA

Development and Testing Environment

A separate stand-alone test environment is an optimal way to reduce risk to the production environment. The development environment allows for the testing of upgrades, potential resolutions, isolation of issues, etc. Cherwell generally allows customers to install copies of the licensed software in non-production environments for purposes of testing, development, or disaster recovery, so long as

such copies are not used for production purposes and the total number of concurrent users in the production environment does not exceed the number of concurrent users authorized under your EULA or EUSA.

Product Knowledge/Training

Cherwell requires system administrators to be equipped with product education and training on Cherwell Service Management. User training is also highly recommended. Cherwell's Professional Services Organization can provide educational options through classroom training at one of Cherwell's corporate locations(s) or through on-site consulting and training options.

Performance Management and System Tuning

Unless Cherwell Software is hosting your instance(s), Cherwell recommends that system administrators monitor performance and disk space availability on a routine basis. As with any system, production environments, performance, and disk space may degrade over time and can result in performance problems or system failures.

Contact Information

Support Website:	www.cherwellsupport.com
Support E-mail:	support@cherwell.com
	camsupport@cherwell.com

Corporate Headquarters — North America

Support Phone:	+1.719.386.7000
Address:	10125 Federal Drive, Suite 100
	Colorado Springs, CO 80908, USA

Europe, the Middle East, and Africa Headquarters

Support Phone:	+44 (0)1793 544899
Address:	Delta 1200, Delta Office Park
	Swindon, Wiltshire, SN5 7XZ

Tab 4) Prior Experience and References

1. Proposer Experience in ITSM

Beyond20 was founded on the belief that IT Services should be measured according to the outcomes they support, and that the technology is not an end unto itself. Processes do not have to be bureaucratic, and good processes can be a powerful enabler.

Beyond20 is first and foremost a process company. We are not only a Cherwell Partner, but also an accredited ITIL Training organization, and frequently conduct ITSM / ITIL consulting engagements. We practice what we preach with 100% of our staff (from developers to marketing) having ITIL Foundations certification, many of whom also have having Intermediate and Expert certifications.

2. Firm Qualifications

Beyond20 has been in business for more than 12 years and is a woman owned, minority owned small business and certified Disadvantaged Business Entity (DBE). Since 2006, our solutions consultants have helped hundreds of organizations across a variety of industries implement ITSM platforms and improve ITIL processes.

We implement and deploy Cherwell Service Management every day (literally). Our experienced team excels at getting the most out of Cherwell, and our solutions built on the Cherwell Service Management Platform have been recognized for their quality.

Cherwell outsources both implementation and consulting services to Beyond20 for engagements they sell directly. This is strong evidence of Cherwell's belief in the quality of the Beyond20 team.

3. Qualified References

Out of respect for the privacy of our customers, it is Beyond20's policy not to publish customer contact and detailed project information in public sector RFP responses. Should you wish to contact any of our customers, please contact Yas Kusakawa at yas.kusakawa@beyond20.com or by phone (202) 448-9073, and we will be happy to provide this information directly.

Customer	Project Description
City of Stockton, CA	We implemented Cherwell Service Management for the City.
City of Detroit, MI	We conducted an ITSM Assessment, Service Catalog Workshop, Workflow Gap Analysis, and implemented Cherwell Service Management for the City.
Municipality of Anchorage, AK	We implemented Cherwell Service Management for the City.

Our Customers

See Appendix E for case studies highlighting our customers' experiences with Beyond20 and Cherwell Service Management, and see below for a sample selection of our customers.

4. Personnel References:

a. Implementation Project Manager

The Project Manager for this engagement will be Lauren Foiles.

Lauren Foiles – Project Manager

As project manager, Lauren will act as the Airport's point of contact for contract related issues, be responsible for scheduling meetings, deliver regular project updates and manages all inquiries related to performance, progress, scheduling, and service.

    Additional Relevant Credentials:
    ITIL Expert
        ITIL v3 Foundations
        ITIL v3 Intermediate Continual Service Improvement (CSI)
        ITIL v3 Intermediate Operational Support and Analysis (OSA)
        ITIL v3 Release, Control and Validation (RCV)
        ITIL Managing Across the Lifecycle
    Certified Scrum Master (CSM) certificate, Scrum Alliance
    Certified Project Management Professional (PMP)

b. Implementation Key Personnel

This engagement will be completed by a Solutions Architect and a Solutions Consultant.

Larry Martin – Solutions Architect

Larry comes with over fifteen years in the field of IT Service management services delivery. Larry's operational experience as a service provider in a complex municipal environment as well as his depth and breadth of industry experience and extensive subject matter expertise in processes, and strategic technology infrastructure planning brings an unmatched understanding and nuance to his development work.

Additional Relevant Credentials:
ITIL v3 Foundations
ITIL Intermediate – Continual Service Improvement (CSI)
Cherwell Certified Implementer®
Cherwell Asset Management Endorsement for Partners v.13.0
Extensive ITSM tool implementation experience in municipal environments

Christian Greenleaf – Solutions Consultant

Christian has considerable experience in implementing Cherwell, including work at a Fortune500 company where he created and automated system workflows and later helped reduce business process times by half. He works as a key part of Beyond20's Professional Services team to develop customer solutions on the Cherwell Service Management Platform.

Additional Relevant Credentials:
ITIL v3 Foundations
ITIL Intermediate – Continual Service Improvement (CSI)
Certified ScrumMaster
Cherwell Certified Implementer®

Tab 5) Concepts and Solutions

1. ITSM Service Management Software Solution Requirements Response Matrix (Attachment A)
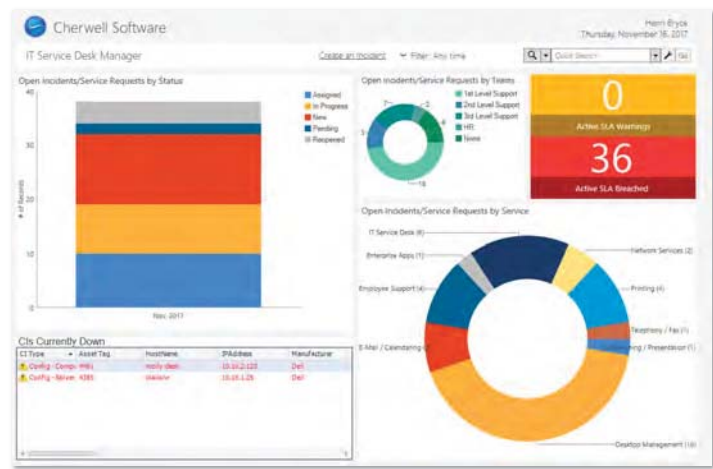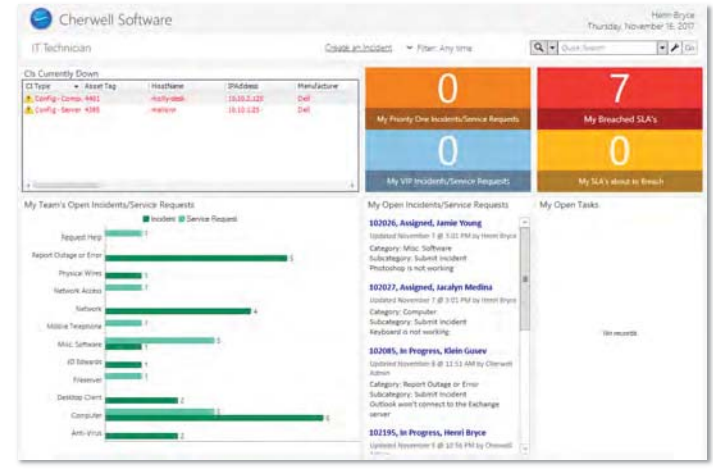
See following pages for the Requirements Response Matrix.

RESPONDENTS SHALL populate the "Level of Compliance" and "Response Code" columns for all Functionality and include comments to explain that functionality, provide additionally information about the functionality, or explain deficiencies in the functionality. Comments should include detailed explanations sufficient to clearly communicate the effort and methodology needed to fulfill the function. References by page and paragraph to attached documents are acceptable.	Level of Compliance: 1 = Fully Compliant (Provide Code) 2 = Partially Compliant (Provide Code) 3 = Not Compliant	Use these codes for Fully/Partially Compliant functions. **Response Code Values:** 1 = Standard feature or add-on priced and included in this proposal 2 = Third Party or add-on, not included in this proposal (reference 3rd party sources) 3 = Configuration 4 = Requires Programming 5 = Planned future functionality within 12 months NA = Not applicable		

Reference	Required Statement / General Functions	Level of Compliance	Response Code	Comments (for Fully/Partially Compliant functions)
	FUNCTIONAL, INTEGRATION, AND TECHNICAL REQUIREMENTS ITIL Compliance: Solution should include functionality that is fully compliant with ITIL v3-2011 for the following process disciplines. Solution should provide fully integrated functionality across the following disciplines. If any capability area is provided by an external 3rd-party product, please name and describe the solution's interface method with the product:			
1	Incident Management	1	1	Out-of-the-box Cherwell provides the features and the flexibility necessary to manage service interruptions in ways that make the most sense for your business. As always in Cherwell, the relationships to other ITIL processes are fully present. Technicians can link an Incident record with records from any other Cherwell business object. You will find the fundamental relationships already there such as the ability to link to Problems, Changes, the CMDB, the people reporting the incident, the Services associated with the interruption, the Service Level Agreements for the process as well as the service affected, etc.
2	Problem Management	1	1	Cherwell supports both reactive and proactive problem management. The system can be configured to recommend a course of action (such as creating a problem) based on metric data and related tickets. The Problem Management business object in Cherwell is focused on three objectives: •Managing multiple incidents related to a Problem including providing workarounds to end users experiencing the issue and resolving related incidents as a group. •Identification of the root cause of the problem. •Eliminating the root cause through Change Management and preserving the process relationship.
3	Request Fulfillment Management	1	1	With Cherwell Service Requests, you may streamline and automate common service requests such as new employee set-up, requests for equipment, etc. End users can easily select the desired service from the service catalog, and track the progress of their request via the self-service portal. Technicians can quickly review, approve, and communicate to end-users the status of the request with Cherwell's simple One-Step actions.
4	Change Management	1	1	Full and formal Change Management that follows the Request for Change (RFC) lifecycle as described in ITIL is an out of the box process in Cherwell. The AirportCity can adopt as much or as little of this formality as is required in their environment using Cherwell's intuitive and codeless administrative toolbox. ITIL-based visual workflows guide you through each core activity of Change Management. Know in advance how changes can impact your assets and eliminate conflicts, both up- and down-stream, with the Visualization Manager (see below). Effortlessly conduct post-change analysis to understand how changes impacted timelines, expenses, or goals with Cherwell's post-implementation questionnaire. Cherwell has an assessment phase in Change Management that allows you to document information about risk, technical analysis, back out plans, acceptance criteria, costs items and full financial impact. These are defined out of the box, but you may add or delete criteria as needed. We have some customers in the Financial Services sector who have a much more detailed risk analysis list, for example. Any additional information can be attached to the record as well.
5	Service Catalog Management	1	1	Managing an IT organization without a Service Catalog is like running a restaurant without a menu. An effective Service Catalog provides a clear means of communicating the services offered to customers and a foundation for meaningful reporting that enables management to effectively manage. Cherwell provides an actionable, easy-to-use service catalog that presents end users with only those specific services to which they are entitled. You can even provide associated costs, estimate delivery times, and leverage product catalogs to enable charge-backs.

6		Service Level Management	1	1	Service Level Management is the process responsible for negotiating achievable service level agreements and ensuring that these are met. It is responsible for ensuring that all IT service management processes, operational level agreements, and underpinning contracts are appropriate for the agreed service level targets. Service level management monitors and reports on service levels, holds regular service reviews with customers, and identifies required improvements. CSM Service Level Management is the process that ensures that Service Level Agreements (SLAs) are carried out appropriately. There are several out-of-the-box Incident and Service Request Metrics available in the Metrics Manager to ensure SLAs are carried out appropriately. Cherwell also makes it easy for organizations to define, implement, and report on metrics specific to them.
7		Knowledge Management	1	1	Reduce service desk requests by providing "Google-like" one-click access to federated knowledge searches of existing modules, PDFs, Microsoft® Office, and URLs. Cherwell's powerful knowledge management features can help your service desk team – and your customers – improve resolution times by providing a repository to successfully capture, structure, and reuse service-related knowledge. A Pink Verified ITIL v3.0 Knowledge Management module is provided out-of-the-box at no additional charge. The Knowledge Management module includes strong metrics and approval capabilities. Cherwell's metrics allow you to run very comprehensive reports on all aspects of Knowledge Management such as usage, relevance and security levels. The Knowledge article Business Object is 100% user-definable and can be populated manually or with packaged content from any 3rd party knowledge vendor.
8		User self-service for request and knowledge management	1	1	The Cherwell Self-Service Portal allows end-users to log in to Cherwell in a browser and create business object such as new knowledge submissions (including attachments), be kept up to date via the notes, and see a history of all business objects created. Additionally, they are able to browse the Knowledge Base, and view frequently accessed documents via the Document Repository.
9		Service Analytics and Reporting	1	1	Cherwell ships with well over 150 pre-defined reports built-in. The reporting engine also allows for limitless custom reports to be built by the client. But it is Cherwell's dashboards that really separate the platform from other tools. Dashboards can be configured to provide real-time reporting in a graphical, easy-to-digest fashion, allowing for drill-down capabilities, metrics—which can provide visual queues and alerts when certain metric criteria are met—and myriad combinations of charts, gauges and specifics search-based results, giving each individual at the data he/she needs instantly in a manner that is most meaningful to him/her. Cherwell dashboards can be configured to show any manner of key performance indicator, whether it be first call resolution, or rate of consumption of a single service type. Because any data point can be mapped and reported on, there is no limit to the types of metrics that can be graphically represented on a dashboard.
	Other ITSM Functional and Technical Requirements: Solution should have the following additional functional and technical capabilities:				
10		The solution provides a role-based graphical user interface that allows different permissions and levels of access	1	1	Cherwell dashboards can be configured to show any manner of key performance indicator, whether it be first call resolution, or rate of consumption of a single service type. Because any data point can be mapped and reported on, there is no limit to the types of metrics that can be graphically represented on a dashboard.
11		The solution provides the capability to add a multiple number of attachments to ticket records	1	1	Multiple attachments can be attached to a ticket record. Attachment file size limits and file type limits can be controlled by the City to meet the City's needs.
12		The solution provides the ability to capture date, time and user id of the person updating the record (the person logged in) for all key events such as assignments, notifications, alerts and so on. The objective of this requirement is to enable various reporting capabilities	1	1	This information is preserved as historical information in the journal tab of the ticket record.
13		The solution provides the ability to create tickets automatically via external tools (e.g. emails, web forms, monitoring and alerting tools)	1	1	Tickets can be created automatically via external tools. This can be done via configuration of an email monitor or other integration methods (e.g. RESTful API, direct database connections).
14		The solution provides the ability for the Assignee to mark the task complete and identify a Task Completion Code and relevant comments	1	1	Employees who are assigned tasks will have the ability to mark a task complete and identify a Task Completion Code and add relevant comments.

15		The solution provides the ability for tasks to proceed in either a serial or parallel (or combination) fashion as defined when the tasks were created. This sequence can be modified prior to their execution if needed	1	1	If you can draw it on a whiteboard, you can build it in Cherwell. Tasks that are kicked off from requests can run sequentially and in parallel; approvals can require 100% of decision maker approval or just a simple majority. This sequence can be modified prior to the execution if necessary.
16		The solution provides out-of-the-box ITIL workflows that are ready to be used or workflows that are configurable	1	1	As noted in the previous section Cherwell Service Management (CSM) technology ships "out-of-the-box" with ITIL workflow and framework built in. CSM is currently PINK verified for the (11) ITIL processes shown below. In this section, we will address how these will meet the City's ITSM needs.
17		The solution provides the ability to search for a ticket via user name, asset id etc. End Users may not always have the Incident number at hand as such searches may have to be performed on the user's ID, name or other keywords associated with the ticket	1	1	Cherwell's full-text search functionality allow for highly specific searches, including filtering by any field, limiting by any date/time, and returning records in any order needed.
18		The solution provides the ability to re-assign the ticket to another support group or individual within the same support group, including automatic notification to the newly assigned group or individual	1	1	CSM can be configured to allow for the re-assigning of a ticket to another support group or individual within the same support group with the transfer triggering automatic notifications to the newly assigned group or individual. This can be set-up with approvals or limited to team leads to ensure tickets are re-assigned properly.
19		Access to the Activity Log is governed by role-based security	1	1	Cherwell's powerful journaling capabilities give the City the ability to control over how much information to store about each ticket. Auditing can be done at the field level, providing a balance between sufficient historical data and data storage efficiency. Additionally, any e-mail sent to or from the system is logged, in its entirety, as a journal entry.

		General			
		The solution supports ITSM process workflow between solutions users including routing of request, electronic request approvals by actionable e-mail, etc.			
20		The solution supports ITIL Version 3 frameworks including terms and definitions	1	1	Cherwell supports 11 ITIL processes out of the box.
21		Solution includes integrated IT Service Operation Management, including Incident, Service Request, Problem, and Change Management	1	1	Cherwell Service Management ships out of the box with Incident Management, Request Fulfillment, Problem Management, and Change Management.
22		Solution includes integrated CMDB (Configuration Management Database) for managing key ITIL V3 functions and processes: IT Service Desk, Incident, Problem, Change, and Service Level	1	1	Cherwell Service Management ships out of the box with a CMDB that is fully integrated with Incident Management, Problem Management, Change Management, and Service Level Management.
23		The solution provides Search capabilities in all ITSM processes – ad hoc queries, save queries, user queries, role-based queries	1	1	CSM provides an extremely powerful search engine and a host of search tools to help technicians efficiently and thoroughly search and filter through CSM data to locate one record or a set or records. This makes it easy to find information such as "all incidents that have server x in their description." It's important to know that any field in Cherwell can be queried and used to filter searches and reports.
24		The solution provides sharing of saved queries including the ability to share to other individuals, groups, and "all" users	1	1	Users will be able to quickly build and save commonly used queries. These can also be shared with teams or across the organization. As noted above, users will able to easily create queries. Within Cherwell, Queries are built using clauses and conditions.
25		The system allows users to rate the quality of service. Please indicate the mechanism for doing this (e.g. embedded form in an email) in the Comments. Also indicate which incidents are chosen for random sampling of feedback (a percentage, a random number per day, etc.)	1	1	The CSM Survey module is configured to send surveys on the completion of an incident or service request. Questions can be added or modified within the client and will immediately take effect on future surveys. Additional specific survey templates (ie: HDI and Net Promoter) are available on the mApp Exchange for integration if you prefer to use a specialized format.
26		Ability to integrate with Maximo (version 7.6 R1) platform	1	3	CSM integrates with numerous applications and technologies via email monitors, direct-database connections, SOAP, and RESTful web-services
27		Ability to integrate with System Center Configuration Manager (SCCM)	1	1	SCCM integrates so that inventory data (ex: workstations, installed programs/software, installed services, disks, etc.) can be shared with and used within the CSM CMDB (as Configuration Item records).
28		Ability to create customizable notifications based on ticket classification	1	1	Different notifications can be sent out based on information within individual tickets.
		Usability			
29		Solution provides dashboard capabilities	1	1	Dashboards provide real-time, at-a-glance view to track important Business Objects and key performance indicators. Information is relevant to each User, Role, or Team vs. a generic Dashboard. CSM Dashboards are completely configurable by you or you can opt to lock down the Dashboard so that everyone on the same Team (like 1st Level Support) must use the same Dashboard. Additionally our Dashboard Viewer can allow a business manager to view a dashboard without using a Cherwell license.
30		Dashboard configuration is user customizable	1	1	Dashboards can be configured by technicians (provided appropriate permissions have been granted).
31		Provide screenshots of included and customized dashboards if applicable. Use the Comments field. No response to Compliance and Response Code fields necessary.			

#					
32	User-specific dashboard; each user can configure viewing content		1	1	User-specific dashboards can be created so that users have immediate access to the information most relevant to them.
33	Navigation (e.g. menus, forms, screens, web pages)		1	1	Cherwell ships out of the box with an easy to use and highly configurable interface.
34	The solution has a mobile app (Include platforms/OS/versions in Comments)		1	1	Cherwell can be access via a modern mobile browser.
35	The solution supports single sign on		1	1	Cherwell supports federated single sign-on integration with any SAML v2.0 compliant centralized authentication system, such as ADFS.
36	The solution supports idle user logoffs		1	1	Cherwell supports automatically logging-off idle users.
37	The solution has a thick client (Describe technical requirements in Comments)		1	1	Cherwell comes out of the box with a thick administrator client, and a thick desktop client. System requirements are noted in #305 under the Technical Requirements tab.
38	The solution has a Web browser-based interface. Provide list of supported browsers in the Comments section.		1	1	CSM works with Internet Explorer 11+ and the current versions of the following browsers: Google Chrome; Firefox; Microsoft Edge; Mac only: Safari. On mobile, CSM works with: Safari on the latest version of iOS (version 11); Chrome on the last two major versions of Android: Nougat (version 7.x) and Oreo (version 8.x).
39	Integration with desktop products (if applicable)		1	1	CSM integrates with numerous applications and technologies via email monitors, direct-database connections, SOAP, and RESTful web-services.
40	Usability features (e.g. tabs, hotkeys, tool tips, widgets, call-outs, color schemes, identification of required fields)		1	1	Ease of use is a key feature of Cherwell Service Management. Complex searches can be built, saved, modified, and shared without having to write SQL queries. Users will be able to build their own One-Steps (automation processes), allowing them to save time on repetitive tasks.

41		Security features - Role-based Access Control	1	1	Cherwell's security model allows for entirely unique user experience based on role. Additionally, functions and operations can be tailored to meet the client's needs, should various roles or groups need specific access to data, where others should have none. Cherwell provides myriad ways to provide a different user experience based on Security Group, Role and team membership. All access can be controlled at the record field level, as well as providing control over access to different parts of the application, based on client requirements. This role-based graphical user interface that allows different permissions and levels of access applies across all modules including Dashboards, Change Management approvals, and Knowledge Management approvals.
42		Electronic forms with built-in logic, such as auto-population of fields, required fields (i.e., fields that, if not filled out, the software doesn't let you submit the form), drop-down menus, specific formats, in-line help (e.g. descriptions, links to process maps and / or procedures, etc.)	1	1	Cherwell supports the auto-population of fields based on pre-determined business rules. For example, if a customer submits a ticket stating that they are having issues with their laptop, the system could auto-populate their device information from the device that they are associated with.
		Knowledge Base			
43		Solution supports the concept of a knowledge base such that resolutions to common problems can be documented and easily searched and accessed within the system (may use wiki application)	1	1	Cherwell will go out and search an unlimited amount of sources for knowledge all at the same time and bring back comprehensive results including current or past Incidents, Problems, Changes, etc. This federated searching is available in both Cherwell Service Management as well as the Customer Self-Service Portal. Promoting Knowledge to your end users via the Self-Service portal is out-of-the box with Cherwell. Cherwell's "federated" knowledge allows that in addition to providing knowledge from the Cherwell knowledge-base, a knowledge search with return knowledge from an unlimited number and type of sources including such sources as: • PowerPoint • Wikis • Intranets • Document repositories • Web Sources (Microsoft TechNet, Google, etc.
44		Knowledge base searches include attachments and documents	1	1	Knowledge base searches will include the name, description, and contents of attachments that have been uploaded in the Attachment Manager.
45		The solution allows users to rate the quality of information in the knowledge base.	1	1	Users will be able to provide feedback on knowledge articles.
46		The solution allows users to provide feedback about issues within the knowledge base. Please indicate in Comments the mechanism used.	1	1	Customers will be able to add a comment to Knowledge Articles to provide feedback.
47		Knowledge base article can be proposed by anyone, but the software should govern the QA and Development process, e.g. the Incident Manager should have ability to approve knowledge base article before it can be published	1	1	Knowledge articles in Cherwell can go through a review and approval process prior to being published to the database.
		Service Level Agreements			
48		Ability to review an SLA for a specific service.	1	1	Cherwell comes out of the box with an SLA workflow. The SLA workflow is broken down into the following phases: **New:** Creator creates a new SLA and assigns ownership. Then, the owner defines the initial details and submits the SLA for planning/development. **Planning (Development):** Owner develops the SLA, including Target Times and Priority Matrix Elements. When ready, the owner activates the SLA. **Active:** SLA is operational in a live environment. Owner periodically assesses the SLA (SLA can be sent back for review/rework or retired if necessary). **Inactive:** SLA is temporarily out of use. Owner periodically assesses the SLA (SLA can be sent back for review/rework or retired if necessary). **Retired:** Expired/out-of-date SLA is retired. Owner can send the SLA back for review/rework, if necessary.
49		Ability to modify an SLA in real-time.	1	1	If the Airport makes changes to the SLAs, technicians and customers will see these updates when they reload Cherwell.
50		Ability to obtain an approval for SLA changes from a customer through an automated means.	1	1	Cherwell supports requiring approvals by key stakeholders prior to implementing new SLAs.
51		Ability to see costs associated with supported SLA.	1	1	Cherwell supports the ability to show costs for particular services based on pre-determined business rules.
52		Ability to print SLA and any subsequent versions for comparison.	1	3	Users will be able to print grids displaying SLA information for comparison with future versions.
53		Ability to modify metrics for which SLA is measured.	1	1	Metrics in Cherwell can be configured to meet the Airport's business needs.

	RESPONDENTS SHALL populate the "Level of Compliance" and "Response Code" columns for all Functionality and include comments to explain that functionality, provide additionally information about the functionality, or explain deficiencies in the functionality. Comments should include detailed explanations sufficient to clearly communicate the effort and methodology needed to fulfill the function. References by page and paragraph to attached documents are acceptable.	Level of Compliance: 1 = Fully Compliant (Provide Code) 2 = Partially Compliant (Provide Code) 3 = Not Compliant	Use these codes for Fully/Partially Compliant functions. Response Code Values: 1 = Standard feature or add-on priced and included in this proposal 2 = Third Party or add-on, not included in this proposal (reference 3rd party sources) 3 = Configuration 4 = Requires Programming 5 = Planned future functionality within 12 months	
Reference	**Required Statement / General Functions**	**Level of Compliance**	**Response Code**	**Comments (for Fully/Partially Compliant functions)**
	FUNCTIONAL, INTEGRATION, AND TECHNICAL REQUIREMENTS ITIL Compliance: Solution should include functionality that is fully compliant with ITIL v3-2011 for the following process disciplines. Solution should provide fully integrated functionality across the following disciplines. If any capability area is provided by an external 3rd-party product, please name and describe the solution's interface method with the product:			
	Incident Management			
54	Ability for technician to input notes and have auto-populate within the incident description	1	1	Fields on a ticket can be set to be auto-populated based on pre-determined busines rules. Technicians will also be able to input notes their individual notes as well.
55	Ability to limit the incident record ticket creation to only Service Desk personnel	1	1	With Cherwell's robust and flexible security model, the Airport will be able to control who has the ability to create incident tickets. This can be limited to Service Desk personnel.
56	Ability to embed, attach, and / or create call scripts for technicians to foster a customer-oriented culture and facilitate incident diagnosis	1	1	Call scripts for technicians can be built into the workflow to foster a customer-oriented culture and facilitate resolution of the incident.
57	Ability to input and append troubleshooting notes within an incident	1	1	Technicians will be able to enter notes into the ticket. These notes can be customer-facing or for internal purposes.
58	Ability for the technician to switch from Incident to Service Request within the same form or screen	1	1	Incidents and Service Requests are part of the same Business Object within Cherwell. Based on the categorization in the Service Catalog, the ticket will be categorized as an Incident or a Service Request.
59	Utilize a "tabbed" layout for entry of incidents	1	1	Customers and technicians will select the appropriate service, category, and subcategory from the service catalog and populate the appropriate specifics form to enter a ticket into Cherwell.
60	Ability to assign incident to external groups for resolution	1	1	Incidents (or its sub-tasks) can be assigned to external groups for resolution.
61	Ability to assign incident ticket number prior to "saving" the incident	1	1	Cherwell supports this out of the box.
62	Ability to append notes to an incident.	1	1	Technicians will be able to append notes to an Incident.
63	Ability to change due dates without having to change priority	1	1	Staff with the proper permissions will be able to update the due dates without changing the priority of a ticket.
64	Ability to update customer information in real-time from the same form or screen used as incident creation. Assumed customer information is populated from Active Directory.	1	1	Customer information from Active Directory can auto-populate the ticket to reduce time spent gathering information.
65	Ability to "resolve" a ticket upon date assignment without closing the ticket	1	1	Once a ticket as ben resolved, it will move to a "Resolved" status prior to moving to a "Closed" status.
66	Ability to associate "orphaned" or duplicate records with the correct customer.	1	1	Cherwell automatically relates all similar classified Incidents/Service Requests, providing a grid list as a tab on each new ticket form; thus, providing the technician with an immediate view into similar/duplicate tickets already in the system. This allows the technician the ability to either immediately close the new ticket as a duplicate, or to identify events with a larger impact, which can lead to declaring major incidents, and thus tracking all similar incidents under the umbrella of a major incident record.
67	Ability to enter customer specific comments or notes related to customer behavior (e.g. ecstatic, accessibility issues, remote worker, etc.)	1	1	The technician will be able to capture the necessary customer information within the tickets.
68	Ability to integrate with and pull data from Active Directory	1	1	Cherwell can integrate with Active Directory or other LDAP 2 or 3 compliant directories to allow for the automated import and update of user accounts. Cherwell natively integrates with Microsoft Active Directory, allowing for scheduled updates to user data, based on changes made within AD. Additionally, Cherwell is capable of integrating with any LDAP compliant user directory, giving you the flexibility to draw from various sources, as necessary.

69	Ability to prevent incident tickets from being automatically generated from integrated software (e.g. don't want monitoring software to auto-generate a ticket each time the system sends an alert)	1	1	This can easily be configured as part of the configuration of the integration.

		Identification & Logging			
70		Ability to log an incident (separate from service request or problem record) and document key information about the incident into an Incident Record which includes the following information:	1	1	
71		Proper description of issue	1	1	Cherwell supports this out of the box.
72		Number of users affected – helps determine the incident priority	1	1	Cherwell can support this information being captured as part of the ticket.
73		Name (VIP status?)	1	1	Cherwell provides a VIP flag for customers out of the box. These customers get a pre-built SLA specific to their status, which can be configured to meet the client's needs.
74		Phone number to contact customer	1	1	Cherwell supports this out of the box. This information can be auto-populated from other sources such as Active Directory.
75		Location (e.g. Home, Gate, Office)	1	1	Cherwell supports this out of the box.
76		Summary of Issue	1	1	Cherwell supports this out of the box.
77		Computer #	1	1	Cherwell supports this out of the box.
78		If Issue With PC, document whether Shared Use or Internal	1	1	Cherwell supports this information being captured within the CMDB. Information from the CMDB can then be used to auto-populate the ticket.
79		Service Level Agreements by customer/service, if applicable	1	1	Cherwell supports this out of the box.
80		Customer expectations -- Services offered and impacted	1	1	Cherwell supports this out of the box.
81		System dependencies (What services does this incident impact?)	1	1	Cherwell supports this out of the box.
82		Guidelines to determine if service request, Break/Fix, how to, etc.	1	1	Cherwell supports this out of the box.
83		Priority Levels	1	1	Cherwell supports this out of the box.
84		Separate field for technician notes that are private to the technicians, i.e., only the technicians can see their notes	1	1	Cherwell supports this out of the box.
85		Allow attachments to be included with ticket	1	1	Cherwell supports this out of the box.
86		Ability to see revision / update history with associated timestamps	1	1	Cherwell supports this out of the box.
87		User cannot edit information and skew data	1	1	Cherwell supports this out of the box.
88		Limit incident description to 350 characters	1	1	Cherwell supports this out of the box. Character limits can be set on fields as necessary.
89		Have ability to pull escalated or de-escalated incidents to use as training opportunities	1	1	Cherwell supports this out of the box.
90		Only Service Desk can assign priority	1	1	Cherwell supports this out of the box.
91		Drop down with SLAs	1	3	Cherwell supports this out of the box.
92		Ability to track incident by customer, service type, status, date, or resolver group.	1	1	Cherwell supports this out of the box.
93		Ability to verify customer information (e.g. previously reported incidents, recent changes to desktop) and tie to change management	1	1	Technicians will be able to verify customer information against the customer profile within Cherwell.
94		Ability to search for existing incidents; help reduce duplicate incident records.	1	1	Cherwell provides, OOTB, a 'similar tickets' relationship, showing all existing requests in the system which match the classification of the current request. Additionally, Cherwell provides visibility into all outstanding requests for the current customer, which can help alleviate the creation of duplicate requests.
95		Ability to generate knowledge article from an incident.	1	1	Technicians will be able submit the resolution method from an Incident to be added to the Knowledgebase if there are no existing Knowledge Articles covering the topic.
96		Ability to provide self-help information to customers (e.g. how to and workaround and allow customers to access incident information such as status) to help reduce call volume and incident resolution cycle time.	1	1	Cherwell ships out of the box with a self-service portal.
97		Ability to link to knowledge base articles for self-service portal	1	1	Incidents can be linked to to Knowledge Articles, similar incidents, an existing problem, known error, RFC and associate CIs.
98		Limit self-service to levels	1	1	Self-service access can be limited as necessary to meet the Airport's business needs.
99		Customers cannot set the priority of the incident	1	1	Cherwell has a fully configurable Priority table, driven by defined Impact and Urgency criteria. SLAs can also be tied to priority selected within the system.
100		Customers can reset passwords	1	3	Customer will be able to reset their passwords with the self-service portal.

101	Customers can describe problem & impact in a text field	1	1	Customers will be provided fields to properly describe the issue they are experiencing.
102	Drop down menu items	1	1	Drop downs for particular fields can be configured as appropriate.
103	Nested list: hardware, software and apps, supporting services	1	1	Necessary hardware, software, application, etc. information can be captured within the Incident ticket.

		Classification			
104		Ability to categorize an incident by business and technical service categorization, defined within the Service Catalog, and ability to link incident management to the Service Catalog	1	1	Incident Management and the Service Catalog are fully integrated within Cherwell Service Management.
105		Ability to assign a priority to an incident, which drives when an incident should be resolved	1	1	Cherwell comes out of the box with the ability to assign a priority to an Incident. The priority of the ticket will drive the SLA.
106		Ability to categorize an incident as a "major" incident and have the incident follow a separate workflow than other incidents	1	1	Cherwell supports a separate workflow for Major Incidents.
107		Ability to group incidents together	1	1	Incidents can be grouped together under a Major Incident.
108		Ability to re-categorize an incident record to the service request record if it is determined that the incident is actually a service request.	1	1	Tickets can be recategorized as necessary. In Cherwell, the subcategory of the ticket will determine whether the ticket is an Incident or a Service Request.
		Initial Support			
109		Ability to search for known errors and problem records to assist in incident resolution	1	1	Technicians and customers will be able to search for known errors and problem records to assist in Incident resolution.
110		Ability to search for similar incidents to assist with incident resolution.	1	1	Cherwell provides, OOTB, a 'similar tickets' relationship, showing all existing requests in the system which match the classification of the current request. Additionally, Cherwell provides visibility into all outstanding requests for the current customer, which can help alleviate the creation of duplicate requests.
111		Search capabilities include metadata / tags	1	1	Cherwell supports the addition of meta-tags.
112		Ability to support the use of diagnostic scripts based upon incident categorization.	1	1	Cherwell supports creating a process which involves diagnostic scripts based on the Incident categorization.
113		Ability to group incidents together to help identify incident trends or major incidents.	1	1	As noted in #110, Cherwell provides, OOTB, a 'similar tickets' relationship, showing all existing requests in the system which match the classification of the current request. Additionally, Cherwell provides visibility into all outstanding requests for the current customer, which can help alleviate the creation of duplicate requests.
114		Ability to link incidents to problem records through search and categorization.	1	1	Technicians will be able to search for Problems to link a particular Incident to.
115		Ability to link incidents to configuration items (down the road)	1	1	The Airport will have the ability ot link Incident tickets to individual or multiple configuraiton items.
116		Ability to whiteboard incidents.	1	1	An internal notes section can be created to allow for different technicians to provide notes and feedback on the Incident.
117		Ability to track and manage information about current outages and events.	1	1	Cherwell support managing information regarding current outages and events.
118		Ability to identify what services are affected based upon incident.	1	1	Creating an Incident in Cherwell will require categorizing the ticket from the Service Catalog. The Incident ticket will be tied to the Service that is selected.
119		Ability to view recent changes to services to help diagnose cause of incident.	1	1	Cherwell supports viewing recent changes (e.g. changes implemented in the past X days) to help diagnose the cause for the Incident. The Incidents can also then be linked to the Changes, so that in the Post-Change Review, the Airport will be able to see the impact of the change.
		Escalation			
120		Ability to functionally assign incidents to resolver groups, using queue management techniques (e.g. assigning incidents to groups and individuals).	1	1	With Cherwell, incoming tickets can be managed in various ways. For example, tickets can be assigned to teams in a round-robin fashion, with individuals picking up tickets from a team queue.
121		Ability to retain Incident Record information from previous steps for resolver groups to view	1	1	Users will be able to view any fields to which they have been granted access.
122		Ability to monitor incident assignment and track incident status.	1	1	The Airport will be able to monitor the progress of open Incidents.
123		Ability to hierarchically escalate an incident, to provide greater visibility and urgency. Ability to support a different workflow based upon escalation of incident.	1	1	Tickets can be escalated manually or automatically based on pre-determined business rules. Depending on the business rules, various notifications can be sent out to make sure all key stakeholders are notified.
124		Ability to support auto assignment based upon categorization.	1	1	Incoming tickets can be auto-assigned based on the ticket categorization. The ticket categorization can also drive the escalation workflow.
125		Ability to support the use of multiple resolver groups.	1	1	Cherwell supports the use of multiple resolver groups. We recommend leveraging sub-tasks to assign tasks to different groups, so that the ticket owner is clearly defined.
126		Ability for Service Desk to view unassigned incidents.	1	1	Technicians will be able to easily search for unassigned Incidents. This can be done via a search, or a widget displaying unassigned tickets can be created for a dashboard.

127	Investigation, Diagnosis, and Resolution	1	1	The Incident workflow is broken down into the following phases: **Detect:** Incident is detected (Portal, call, e-mail, automated). This phase is not tracked in CSM. **Record:** Creator logs a new Incident. Then, creator records the initial Who (Requestor), What (Description), and How (Call Source) details. **Classify:** Creator classifies the Incident (Service/Category/Subcategory, Priority, Major Incident, and CI). **Investigate (Incident) or Fulfill (Request):** Ownership is assigned. Owner investigates or diagnoses the Incident or fulfills the Request. (Owner creates/assigns Tasks to one or more Task owners, if needed.) When a resolution is diagnosed/fulfilled, owner resolves the Incident/Request (records resolution details and code). **Resolve:** Owner submits resolution to the Knowledge Base (as Knowledge Article), if necessary. Owner can also close the record (to finalize the process) or reopen the record (to make changes). **Closed:** Closed Incident/Request can be searched and viewed, but not edited.	
128	Ability to document incident resolution			Technicians will be able to document the resolution of the Incident and even submit the resolution method to be added to the Knowledgebase if there are no existing Knowledge Articles covering the topic.	
129	Allow service desk personnel and resolver groups ability to update the ticket	1	1	Service desk personnel and resolver group will have the ability to update the ticket as necessary.	
130	Ability to update incidents, tracking users, and date/time of update.	1	1	Cherwell's powerful journaling capabilities will capture who/when made particular updates to the incident.	
131	Ability to tie resolutions to known errors.	1	1	Resolved tickets can be tied to known errors.	
132	Ability to search resolutions and provide resolution information to Service Desk to reduce time to resolve.			Resolved tickets can be searched to provide service desk with resolution information to the Service Dek and reduce the time it takes to resolve a ticket.	
133	Ability to monitor incident progress and presort on outstanding incidents.	1	1	The Airport will be able to monitor the progress of open Incidents.	
134	Ability to create a problem record from an incident record.	1	1	Technicians will be able to create a Problem record from an Incident record.	
135	Ability to track mean time to resolve.	1	1	Cherwell supports this out of the box.	

		Closure			
136		Ability to review resolved incidents.	1	1	Staff will be able to review closed tickets.
137		Ability to track mean time to close.	1	1	Cherwell supports this out of the box.
138		Ability to perform quality control on resolved incidents.	1	1	The Airport will be able to review resolved incidents for quality control purposes. For example, supervisors may want to review tickets for which a customer survey yielded negative feedback.
139		Ability to report on incident by status.	1	1	Staff will be able to report on any fields to which they have access, including the status of incidents.
140		Ability to automatically close a ticket after resolution (e.g. 48 hours), during which a ticket can be re-opened for editing	1	1	Incident tickets can be set to automatically close after a set amount of time following resolution.

| | RESPONDENTS SHALL populate the "Level of Compliance" and "Response Code" columns for all Functionality and include comments to explain that functionality, provide additionally information about the functionality, or explain deficiencies in the functionality. Comments should include detailed explanations sufficient to clearly communicate the effort and methodology needed to fulfill the function. References by page and paragraph to attached documents are acceptable. | Level of Compliance:
1 = Fully Compliant (Provide Code)
2 = Partially Compliant (Provide Code)
3 = Not Compliant | Use these codes for Fully/Partially Compliant functions.
Response Code Values:
1 = Standard feature or add-on priced and included in this proposal
2 = Third Party or add-on, not included in this proposal (reference 3rd party sources)
3 = Configuration
4 = Requires Programming
5 = Planned future functionality within 12 months
NA = Not applicable | | |

Reference	Required Statement / General Functions	Level of Compliance	Response Code	Comments (for Fully/Partially Compliant functions)
	FUNCTIONAL, INTEGRATION, AND TECHNICAL REQUIREMENTS *ITIL Compliance: Solution must include functionality that is fully compliant with ITIL v3-2011 for the following process disciplines. Solution must provide fully integrated functionality across the following disciplines. If any capability area is provided by an external 3rd-party product, please name and describe the solution's interface method with the product:*			
	Problem Management			
141	Ability to track known errors.	1	1	Cherwell's Problem Management module supports tracking Known Errors.
142	Ability to track problem records.	1	1	Cherwell supports the full lifecycle of Problem Management.
143	Ability to assign problem records to resolver groups and individuals (both internal and external to ABIA Information Systems).	1	1	Problem records can be assigned to groups / individuals both internal and external ABIA Information Systems. All staff who will be updating the Problem record in the system will need to be a Cherwell user.
144	Ability to proactively manage identified problems.	1	1	Cherwell supports both reactive and proactive problem management. The system can be configured to recommend a course of action (such as creating a problem) based on metric data and related tickets.
145	Ability to identify and track repeat problems.	1	1	Open incidents can be tied to Known Errors (or a new Problem) so that the Airport will have visibility into the impact of the Problem.
146	Ability to assign Key Performance indicators and measures against those KPIs.	1	1	This is supported OOTB.
147	Ability to create and manage problem records.	1	1	Cherwell supports the full lifecycle of Problem Management.
148	Ability to link problem records to incidents.	1	1	Problem records can be linked to Incidents.
149	Ability to document and share known errors to improve incident resolution.	1	1	With Cherwell, the Airport will be able to document known errors and workaround and share the necessary information with technicians and customers.
150	Ability to integrate knowledge base articles into system	1	1	Cherwell supports the full lifecycle of Knowledge Management.
151	Ability to search problem records by metadata / tags	1	1	Cherwell supports the addition of meta-tags.
152	Ability to incorporate / integrate problem records and knowledge articles need to be integrated into system	1	1	All of Cherwell ITIL processes are fully integrated - this includes Problem Management and Knowledge Management.
153	IS staff permission to open problem ticket	1	1	With Cherwell's robust and flexible security model, the Airport will be able to control who has the ability to open Problem tickets.
154	Counter on master ticket for all the tickets are linked	1	1	Cherwell supports having a counter of all associated tickets.
155	Build in logic that pares down resolver group options based on the symptoms recorded	1	1	How the Problem record is routed can based on pre-determined business rules.
156	Dashboard alerting that's color coded to reflect status update	1	1	Dashboard widgets / displays can be color coded to reflect status updates.
157	Ability to modify master ticket based on final root cause	1	1	Once a root cause has been determined and the Problem resolved, the Airport will have the ability to automatically close all associated tickets.
158	Ability to create symptom tags and create notifications when new symptoms arise	1	1	Cherwell supports creating symptions tags for Problem records, with the addition of new symptoms, triggering notifications to the appropriate stakeholders.
159	Ability to create and send updates to/from the Service Desk that includes the following information:			

160	Incidents they can expect to see	1	1	Cherwell supports sending notifications with this information.
161	Update – time to resolution	1	1	Cherwell supports sending notifications with this information.
162	Resolver point of contact	1	1	Cherwell supports sending notifications with this information.
163	Notify customer of activity	1	1	Cherwell supports sending notifications with this information.
164	Acknowledge that their problem is being worked on	1	1	Cherwell supports sending notifications with this information.
165	Notification of impending outage	1	1	Cherwell supports sending notifications with this information.
166	Banner on self-service portal with alerts and notifications	1	1	Cherwell supports sending notifications with this information.
167	Ability to create an After-Action Review that includes the following sections:			
168	Symptoms of the problem	1	1	Cherwell supports having a Problem Review process that includes this information.
169	Assessment of the impact of the problem	1	1	Cherwell supports having a Problem Review process that includes this information.
170	All root causes investigated (including those that weren't found to be the actual root cause)	1	1	Cherwell supports having a Problem Review process that includes this information.
171	Any information related to the workaround (if no workaround pursued, this should be documented as well)	1	1	Cherwell supports having a Problem Review process that includes this information.
172	All actions taken to resolve the problem (or reason why resolution was not pursued/implemented)	1	1	Cherwell supports having a Problem Review process that includes this information.
173	Any lingering questions or potential red flags (e.g. something that may indicate the problem is returning)	1	1	Cherwell supports having a Problem Review process that includes this information.
174	Any follow-up actions required as a result of the problem resolution	1	1	Cherwell supports having a Problem Review process that includes this information.
175	Diagnostic scripts for the Service Desk to reference in the future as needed or appropriate	1	1	Cherwell supports having a Problem Review process that includes this information.

REPORTING REQUIREMENTS

	RESPONDENTS SHALL populate the "Level of Compliance" and "Response Code" columns for all Functionality and include comments to explain that functionality, provide additionally information about the functionality, or explain deficiencies in the functionality. Comments should include detailed explanations sufficient to clearly communicate the effort and methodology needed to fulfill the function. References by page and paragraph to attached documents are acceptable.	Level of Compliance: 1 = Fully Compliant (Provide Code) 2 = Partially Compliant (Provide Code) 3 = Not Compliant	Use these codes for Fully/Partially Compliant functions. Response Code Values: 1 = Standard feature or add-on priced and included in this proposal 2 = Third Party or add-on, not included in this proposal (reference 3rd party sources) 3 = Configuration 4 = Requires Programming 5 = Planned future functionality within 12 months NA = Not applicable

Reference	Required Statement / General Functions	Level of Compliance	Response Code	Comments (for Fully/Partially Compliant functions)
	FUNCTIONAL, INTEGRATION, AND TECHNICAL REQUIREMENTS ITIL Compliance: Solution should include functionality that is fully compliant with ITIL v3-2011 for the following process disciplines. Solution should provide fully integrated functionality across the following disciplines. If any capability area is provided by an external 3rd-party product, please name and describe the solution's interface method with the product:			
	REPORTING REQUIREMENTS (ITSM METRICS / REPORTS)			
246	Ability to filter by specific time periods: daily, weekly, monthly, 12 days, ad hoc	1	1	The Airport will be able to filter based on the specific time periods.
246	Ability to filter by groups and individual FTE	1	1	The Airport will be able to filter based on gouprs, individuals, etc.
246	Ability to ensure a high fidelity to data, i.e., users cannot manually override time stamps to adjust / skew data	1	1	Whether or not fields can be editted / updated can easily be set by the Airport. With Cherwell's powerful journaling capability, the Airport will be able to look into changes that have been made to individual fields.
246	Ability to capture and report the following metrics and KPIs:			CSM ships out of the box with many useful metrics that the Airport can leverage to gain visibility and understanding of the state of your service desk. Cherwell's metrics allow you to run very comprehensive reports on different work being tracked in Cherwell. This can be used to measure, monitor, and predict metrics including but not limited toInput, Output, Status, Timeline, Thresholds, Satisfaction, Success Trends, Cause, Performance, and Averages.
	Incident Management Metrics & **KPIS**			
247	Total number of incidents	1	1	This is supported OOTB.
248	Total number of self-service incidents	1	1	This is supported OOTB.
249	Total number of emails to the service desk	1	1	This is supported OOTB.
250	Number of incidents re-opened	1	1	This is supported OOTB.
251	Number of incidents per user	1	1	This is supported OOTB.
252	Total number of incidents by IT Service & Priority	1	1	This is supported OOTB.
253	Percentage of incidents closed at the Service Desk	1	1	This is supported OOTB.
254	Percentage of incidents escalated to a resolver group	1	1	This is supported OOTB.
255	Percentage of incidents escalated to a resolver group that could have been resolved by the Service Desk	1	1	This is supported OOTB.
256	Mean time to resolve incidents	1	1	This is supported OOTB.
257	Total labor hours spent resolving incidents (specific to resolver groups)	1	1	This is supported OOTB.
258	Incidents resolved by individual staff (normalized for work availability)	1	1	This is supported OOTB.
259	Average number of incidents resolved by FTE in a month	1	1	This is supported OOTB.
260	Average user satisfaction survey score	1	1	This is supported OOTB.

261	Incident backlog / incidents opened past SLA per Service, or percentage of SLAs not met by IS	1	1	This is supported OOTB.
262	Cost per incident	1	1	This is supported OOTB.

	Problem Management Metrics and KPIs				
263	Number of known errors documented vs. problems resolved	1	1	This is supported OOTB.
264	Percentage of incidents resolved at the Service Desk using known error documentation	1	1	This is supported OOTB.
265	Current problem record backlog by IS Service	1	1	This is supported OOTB.
266	Number of repeat incidents or number of incidents per IS Service linked to a problem record	1	1	This is supported OOTB.
267	Number of problem records by priority (including major problems)	1	1	This is supported OOTB.
268	Total number of problems	1	1	This is supported OOTB.
269	Mean time to resolve for incidents linked to problem record	1	1	This is supported OOTB.
270	Number of problems resolved within agreed service levels	1	3	This is supported OOTB.
271	Number of incidents per problem record	1	1	This is supported OOTB.
	Service Request Fulfillment Metrics and KPIs				
272	Mean time to fulfill service request by service item	1	1	This is supported OOTB.
273	Number of service requests by phase	1	1	This is supported OOTB.
274	Level of user satisfaction with how the service request was fulfilled	1	1	This is supported OOTB.
275	Total number of incidents related to service request activity	1	1	This is supported OOTB.
276	Service requests fulfilled (or in progress) that are past agreed to SLA	1	1	This is supported OOTB.
277	Total number of service requests	1	1	This is supported OOTB.
278	Total work effort required to fulfill service request	1	1	This is supported OOTB.
279	Percentage of backlogged service requests	1	1	This is supported OOTB.
	Change Management Metrics and KPIs				
280	Number and percent of incidents attributed to a change	1	1	This is supported OOTB.
281	Number and percent of changes that are categorized as emergency changes	1	1	This is supported OOTB.
282	Number and percent of unauthorized changes	1	1	This is supported OOTB.
283	Number and percent change in discrepancies in CMDB	1	1	This is supported OOTB.
284	Number of changes by working group	1	1	This is supported OOTB.
285	Number of unauthorized changes	1	1	This is supported OOTB.
286	Ratio of number of incidents vs. number of changes	1	1	This is supported OOTB.
287	Percentage of changes caused by incidents	1	1	This is supported OOTB.
288	Percentage of changes initiated by customers	1	1	This is supported OOTB.
289	Number of changes by change type	1	1	This is supported OOTB.

290	Percentage of unplanned outages due to changes	1	1	This is supported OOTB.
291	Number of incidents linked to recent change	1	1	This is supported OOTB.
292	Percentage of unplanned outages due to changes	1	1	This is supported OOTB.
293	Number of incidents linked to recent change	1	1	This is supported OOTB.
294	Percentage of incidents linked to recent change	1	1	This is supported OOTB.
295	Percentage of outages due to changes	1	1	This is supported OOTB.
296	Percentage of emergency / urgent changes	1	1	This is supported OOTB.
297	Percentage of unauthorized changes	1	1	This is supported OOTB.

CHANGE MANAGEMENT

	RESPONDENTS SHALL populate the "Level of Compliance" and "Response Code" columns for all Functionality and include comments to explain that functionality, provide additionally information about the functionality, or explain deficiencies in the functionality. Comments should include detailed explanations sufficient to clearly communicate the effort and methodology needed to fulfill the function. References by page and paragraph to attached documents are acceptable.	Level of Compliance: 1 = Fully Compliant (Provide Code) 2 = Partially Compliant (Provide Code) 3 = Not Compliant	Use these codes for Fully/Partially Compliant functions. Response Code Values: 1 = Standard feature or add-on priced and included in this proposal 2 = Third Party or add-on, not included in this proposal (reference 3rd party sources) 3 = Configuration 4 = Requires Programming 5 = Planned future functionality within 12 months NA = Not applicable
Reference	**Required Statement / General Functions**	**Level of Compliance**	**Response Code**	**Comments (for Fully/Partially Compliant functions)**

Reference	Required Statement / General Functions	Level of Compliance	Response Code	Comments (for Fully/Partially Compliant functions)
	FUNCTIONAL, INTEGRATION, AND TECHNICAL REQUIREMENTS *ITIL Compliance: Solution should include functionality that is fully compliant with ITIL v3-2011 for the following process disciplines. Solution should provide fully integrated functionality across the following disciplines. If any capability area is provided by an external 3rd-party product, please name and describe the solution's interface method with the product:*			
	Change Management			
176	Ability to monitor changes.	1	1	Full and formal Change Management that follows the Request for Change (RFC) lifecycle as described in ITIL is an out of the box process in Cherwell. The Airport can adopt as much or as little of this formality as is required in their environment using Cherwell's intuitive and codeless administrative toolbox.
177	Ability to identify specific configuration items slated for change.	1	1	Configuration Item(s) can be tied to RFCs.
178	Ability to identify the services affected by the change.	1	1	Services can be tied to RFCs.
179	Ability to incorporate ABIA-specific change procedures into change management workflow.	1	1	As noted in in #176, full and formal Change Management that follows the Request for Change (RFC) lifecycle as described in ITIL is available in Cherwell. This can be configured to incorporate ABIA's specific change procedures (e.g. approval process, CABs) .
180	Ability to notify CAB members of needed changes and solicit approval or denial of a change.	1	1	CAB can be notified of pending approvals, with follow-up emails sent if they are not responded to within a particular timeframe. With Cherwell, approvers will also have the ability to response to pending approvals via email - which would not require a license.
181	Ability to generate notifications that are disseminated airport-wide.	1	1	Organization-wide notifications can be generated from Cherwell.
182	Ability to notify specific users/groups of the affected services.	1	1	Cherwell can support specific users / groups being notified when a Change is being made to a particular service.
183	Ability to create a Change Request that includes the following information:			
184	Date and time of submittal	1	1	This is supported by Cherwell.
185	RFC Identification #	1	1	This is supported by Cherwell.
186	Status of ticket	1	1	This is supported by Cherwell.
187	Team members involved in change	1	1	This is supported by Cherwell.
188	Change description	1	1	This is supported by Cherwell.
189	What	1	1	This is supported by Cherwell.
190	Proposed date of change	1	1	This is supported by Cherwell.
191	Scope	1	1	This is supported by Cherwell.
192	Systems involved / affected	1	1	This is supported by Cherwell.
193	Downtime	1	1	This is supported by Cherwell.
194	Requester & contact info	1	1	This is supported by Cherwell.

195	Risk to the environment	1	1	This is supported by Cherwell.
196	Impact	1	1	This is supported by Cherwell.
197	Who's impacted	1	1	This is supported by Cherwell.
198	# users	1	1	This is supported by Cherwell.
199	Change type	1	1	This is supported by Cherwell.
200	Change source	1	1	This is supported by Cherwell.
201	Categorization by service	1	1	This is supported by Cherwell.
202	Implementation Plan	1	1	This is supported by Cherwell.
203	Roll back plan	1	1	This is supported by Cherwell.
204	Test plan	1	1	This is supported by Cherwell.
205	Post-implementation / validation plan	1	1	This is supported by Cherwell.
206	Schedule	1	1	This is supported by Cherwell.
207	Links to problem record & incident record	1	1	Change records can be tied to Problem and Incident records.
208	Anyone in IS can submit change request	1	1	With Cherwell's robust and flexible security model, the Airport will be able to control who has the ability to submit change requests.
209	Alert for conflicting change dates & configurable blackout dates	1	1	With the Change Calendar, the Airport will be able to view conficting changes dates as well as check for blackout dates.
210	Threshold option for # changes by change type / group / date	1	1	Cherwell ships out of the box with three types of Changes (Standard / Normal / Emergency). These can be routed differently and have different requirements based on pre-determined business rules.
211	Logic based on severity	1	1	Priorities (Low, Normal, High, or Urgent - or categorizations determined by the Airport) can be set on Changes. These changes can be routed / processed differently based on their priorities and the pre-determined business rules.
212	Change types route to appropriate personnel for approval	1	1	RFCs can be routed to the appropriate personnel for approval.
213	Normal medium / high changes route to CAB and supervisor of the requester linked in AD	1	1	Normal medium / high changes can be routed to the CAB and supervisor of the requestor (with supervisor information pulled from Active Directory).
214	Capture who authorizes change and when change is authorized	1	1	Who authorized what Changes and when those approvals were made will be logged as part of the Change request.
215	Comments section: If request is rejected or canceled, should fill out reason for cancelation	1	1	Filling out a reason for rejecting an RFC can be set to be required.
216	Re-send approval notification to supervisor if she has not made a decision within 48 working hours	1	1	Follow-up notifications can be sent to approvers if a decision has not been made within a certain time frame.
217	Emailed notification / posted notification after CAB meeting 12pm on Tuesdays	1	1	Notifications and posting can be scheduled.
218	System or change coordinator notifies requester, supervisor and change coordinator that change was approved	1	1	Cherwell supports the appropriate stakeholders being notified when a Change is approved.

219	*Dashboard notification day before change is scheduled to occur	1	3	A dashboard can be set to display changes that will be occurring in the near future.
220	Ability to set change window (e.g. 30 days)	1	1	A change window can be set within Cherwell.
221	Notification or flag when 30-day change window expires	1	1	Automated notifications can be sent with a change window expires.
222	System or change coordinator notifies requester, supervisor and change coordinator that change was canceled	1	1	Cherwell supports the appropriate stakeholders being notified when a Change is cancelled.
223	Comments section	1	1	Cherwell's Change Form ships with a Comments field where stakeholders will be able to provide feedback.

SERVICE REQUEST FULFILLMENT

		Level of Compliance:	Use these codes for Fully/Partially Compliant functions.
RESPONDENTS SHALL populate the "Level of Compliance" and "Response Code" columns for all Functionality and include comments to explain that functionality, provide additionaly information about the functionality, or explain deficiencies in the functionality. Comments should include detailed explanations sufficient to clearly communicate the effort and methodology needed to fulfill the function. References by page and paragraph to attached documents are acceptable.		1 = Fully Compliant (Provide Code) 2 = Partially Compliant (Provide Code) 3 = Not Compliant	Response Code Values: 1 = Standard feature or add-on priced and included in this proposal 2 = Third Party or add-on, not included in this proposal (reference 3rd party sources) 3 = Configuration 4 = Requires Programming 5 = Planned future functionality within 12 months NA = Not applicable

Reference	Required Statement / General Functions	Level of Compliance	Response Code	Comments (for Fully/Partially Compliant functions)
	FUNCTIONAL, INTEGRATION, AND TECHNICAL REQUIREMENTS ITIL Compliance: Solution should include functionality that is fully compliant with ITIL v3-2011 for the following process disciplines. Solution should provide fully integrated functionality across the following disciplines. If any capability area is provided by an external 3rd-party product, please name and describe the solution's interface method with the product:			
	Service Request Fulfillment			
224	Ability for personnel within multiple resolver groups to update a service request independent of request ownership.	1	1	Staff with the appropriate permissions will be able to update service request that he or she does not own. The Airport will have control over who is able to make these changes.
225	Ability to quickly change ownership of a request while in-progress.	1	1	Ownership of a ticket can be changed as necessary. This ability can be limited ot team lead or supervisor level users to prevent tickets from being passed around without being resolved.
226	Ability to assign an employee self-service request to a resolver group by default based on request type.	1	1	Cherwell can be configured to automatically route and assign tickets based on selections made in the Service Catalog when submittng the ticket.
227	Ability to have all request features presented to the user.	1	1	What features / fields a user has access to can be granularly controlled by the Airport.
228	Ability to generate, track, and update self-generated tickets.	1	1	This is supported OOTB.
229	Ability for a user to update a ticket once it has been submitted for processing.	1	1	Customers and technicians will be able to submit updates to tickets after it has been submitted.
230	Ability for the system to generate a feedback survey, with the capability of distributing it randomly, at the close of a request.	1	1	The CSM Survey module is configured to send surveys on the completion of an incident or service request. Questions can be added or modified within the client and will immediately take effect on future surveys. Additional specific survey templates (ie: HDI and Net Promoter) are available on the mApp Exchange for integration if you prefer to use a specialized format.
231	Ability to have real-time updated applied to the service catalog.	1	1	If the Airport makes changes to the Service Catalog, technicians and customers will see these updates when they reload Cherwell.
232	Ability to support business services.	1	1	Cherwell's service request module can be used to support business services.
233	Ability to support technical services.	1	1	Cherwell's service request module can be used to support technical services.
234	Ability to support the many-to-many relationships between business and technical services.	1	1	Services in Cherwell can have many-to-many relationships.
235	Ability to support the entitlements of users to make service requests and/or have them approved.	1	1	With Cherwell's robust and flexible security model, the Airport will be able to control who has the ability to make requests as well as particular approvals.
236	Ability to employee role-based access.	1	1	Cherwell supports role-based access. See Appendix B) Cherwell Application Security Whitepaper for additional information.
237	Ability to display or hide costs.	1	1	The Airport will have granular control over whether particular fields (such as costs) are visible to a particular customer or user.
238	Ability to display or hide the SLA associated with a service.	1	1	The Airport will have granular control over whether particular fields (such as SLAs) are visible to a particular customer or user.
239	Ability to support the financial management of service requests via integration with Maximo	1	3	CSM integrates with numerous applications and technologies via email monitors, direct-database connections, SOAP, and RESTful web-services.
240	Ability to incorporate / embed Shared Tenant Service (STS) service request form (unit price calculation with fixed and variable prices), route to appropriate stakeholders, electronically sign, and attach signed STS service request form to work order	1	3	Costs can be tied to particular services so that the necessary stakeholders will have visibility into the costs for a particular request. This can be managed within ths system, or via an form attachment to the ticket.

241	Ability for customers to reset their own passwords from a lockout	1	1	Customers will have the ability to reset their own passwords.
242	A. Include reference to knowledge base or link to instructions for the user on how to reset their own password	1	1	The Airport will have the ability to direct customers to a knowledge article showing them how to reset their password.
243	B. 2-factor authentication or challenge questions	1	2	
244	The solution offers a self-service portal that allows customers to initiate service requests, find information, register, and resolve issues	1	1	Cherwell comes out of the box with a fully configurable Self-Service Portal that supports organizational branding, providing users with a more seamless interaction. The Cherwell Service Management's Portal Client resolves a number of common pain points and offers the following key functionality: •Serve multiple customers, locations, constituents, etc. from one system. •Submit and check status of their Requests avoiding calls requesting updates •View and edit records (approvals, add comments, withdraw requests, etc.). •Anytime, anywhere access using any modern browser, tablet, or mobile device. •Help users to help themselves.
245	The solution allows self-service users to report, comment on, and obtain status on tickets without additional licensing	1	1	Customers using the self-service portal do not consume a license.

RESPONDENTS SHALL populate the "Level of Compliance" and "Response Code" columns for all Functionality and include comments to explain that functionality, provide additionaly information about the functionality, or explain deficiencies in the functionality. Comments should include detailed explanations sufficient to clearly communicate the effort and methodology needed to fulfill the function. References by page and paragraph to attached documents are acceptable.	Level of Compliance: 1 = Fully Compliant (Provide Code) 2 = Partially Compliant (Provide Code) 3 = Not Compliant	Use these codes for Fully/Partially Compliant functions. **Response Code Values:** 1 = Standard feature or add-on priced and included in this proposal 2 = Third Party or add-on, not included in this proposal (reference 3rd party sources) 3 = Configuration 4 = Requires Programming 5 = Planned future functionality within 12 months NA = Not applicable

Reference	Required Statement / General Functions	Level of Compliance	Response Code	Comments (for Fully/Partially Compliant functions)
	FUNCTIONAL, INTEGRATION, AND TECHNICAL REQUIREMENTS ITIL Compliance: Solution should include functionality that is fully compliant with ITIL v3-2011 for the following process disciplines. Solution should provide fully integrated functionality across the following disciplines. If any capability area is provided by an external 3rd-party product, please name and describe the solution's interface method with the product:			
	Technical Requirements			
298	The solution has the ability to add custom fields	1	1	Custom fields can easily be added into Cherwell. Creating new fields is as simple as dropping them onto a form and labeling them. There are a wide variety of field's types available such as date/time, check box. Pick list, integer, text etc.
299	Custom fields are searchable	1	1	All fields within Cherwell are searchable.
300	Custom fields searchable	1	1	All fields within Cherwell are searchable.
301	The solution integrates with Office 365	1	3	CSM natively integrates with Microsoft Exchange.
302	The solution integrates with Identity and Access Management solutions (password management, user provisioning). Provide additional details in the Comments section.	1	1	Cherwell can integrate with Active Directory or other LDAP 2 or 3 compliant directories to allow for the automated import and update of user accounts. Cherwell natively integrates with Microsoft Active Directory, allowing for scheduled updates to user data, based on changes made within AD. Additionally, Cherwell is capable of integrating with any LDAP compliant user directory, giving you the flexibility to draw from various sources, as necessary. Cherwell integrates natively with Active Directory and supports federated single sign-on integration with any SAML v2.0 compliant centralized authentication system, such as ADFS.
303	The solution integrates with Cisco IP phones. Provide additional details in the Comments section	1	3	CSM integrates with all Telephony Application Programming Interface (TAPI)-compliant telephony clients. (The TAPI is a Microsoft Windows API that provides Computer Telephony Integration (CTI) and enables PCs running Microsoft Windows to use telephone services). This includes major providers of telephony services like Avaya, Cisco - Call Manager, and in Contact - ACD/IVR to provide features like auto-population of tickets based on caller ID, screen pop-ups of Customer Records and click-to dial capability.
304	The solution has an open Application Programming Interface (API)	1	1	Cherwell provides a full-featured RESTful API for consumption by external applications and services. Additionally, Cherwell is capable of consuming both SOAP and RESTful web service APIs, allowing for bi- directional integration with external applications and data sources.

305	Provide specific hardware requirements for an on-premise solution (if applicable). Include High Availability and Disater Recovery options for the solution. Use the comments field for this reponse. Level of compliance and Response codes not needed.	N/A	N/A	**Client Minimum Requirements:** **System Processor:** Dual Core CPU or equivalent (1) **System Memory:** 3 GB (4 GB or more recommended) **Operating System:** Windows 10, Windows 8/8.1 x86 or x64 Pro or Enterprise editions, or Microsoft Windows 7 Service Pack 1 (SP1), x86 or x64 editions **Free Disk Space:** Minimum: 1.5 GB (2 GB recommended) **Networking:** Internet Access required for online documentation feature **Browser:** Internet Explorer 11+ and the current versions of the following browsers: Google™ Chrome™, Firefox, Microsoft Edge, Safari (Mac only) (required for Browser applications) **Other:** Microsoft
				Server Minimum Requirements: **System Processor:** Dual Core CPU or equivalent (1) **System Memory:** 4 GB (6 GB or more recommended). Note that if you have SQL Server® installed on the same server, more RAM is recommended. **Operating System:** Windows Server 2016, Windows Server 2012 R2, Windows Server 2012, or Microsoft Windows Server 2008 R2 **Free Disk Space:** Minimum: 5 GB, Recommended: 10 GB **Networking**: Dual Core CPU or equivalent (1)Internet access required for online documentation feature **Database:** Microsoft SQL Server 2016, Microsoft SQL Server 2014, Microsoft SQL Server 2012, or Microsoft SQL Server 2008 R2. Database can be on a separate server. *Note:* Full-text indexing must be enabled. Requires SQL Standard Edition (minimum), either a Processor License or a Server License with sufficient number of Client Access licenses **Other:** Microsoft .NET 4.5.2+; IIS 7.0+ (required for Web Applications and when hosting the Cherwell Application Server in IIS) (2)
				Note: (1) Recent model required. (2) If you host the Cherwell Application Server in IIS, Windows Communication Foundation (HTTP and Non-HTTP Activation) components are also required.
306	Provide specific requirements for a Cloud-based implementation of the solution, if applicable. Use the comments field for this reponse. Level of compliance and Response codes not needed.	N/A	N/A	See #305 for requirements for accessing the desktop client and the browser client.

2. Solution Overview

a. Module and Module Integrations

IT Service Desk Features

Cherwell ships out of the box with 11 ITIL-verified processes. The following are highlights of the features the Airport is looking to implement.

Incident Management

Incident Management is core to any IT Service Management solution. Out-of-the-box Cherwell provides the features and the flexibility necessary to manage service interruptions in ways that make the most sense for your business.

As always in Cherwell, the relationships to other ITIL processes are fully present. Technicians can link an Incident record with records from any other Cherwell business object. You will find the fundamental relationships already there such as the ability to link to Problems, Changes, the CMDB, the people reporting the incident, the Services associated with the interruption, the Service Level Agreements for the process as well as the service affected, etc.

The out-of-the-box UIs are clean and intuitive; they are organized by the execution steps and there is judicious use of tabs to guide the user to the next required steps for the Incident.

Problem Management

Cherwell supports both reactive and proactive problem management. The system can be configured to recommend a course of action (such as creating a problem) based on metric data and related tickets.

The Problem Management business object in Cherwell is focused on three objectives:

- Managing multiple incidents related to a Problem including providing workarounds to end users experiencing the issue and resolving related incidents as a group.
- Identification of the root cause of the problem.

- Eliminating the root cause through Change Management and preserving the process relationship.

One can easily create a problem from a group of related incidents, continue to relate new incidents as they come in during a crisis, maintain the relationships between them, and manage them as one all the way through to resolution through the problem interface. If a change to infrastructure is required in the resolution to that problem, a request for change can be initiated from the problem record and stay related to it. Once a problem has been identified, Cherwell can rapidly communicate problem details to your end users.

Cherwell can also set known outages, configure rules for alerts and stopping alerts as needed. Problems can be linked to automated notifications (both through e-mail/messaging, as well as within notification widgets on dashboards and in the Self-Service Portal), providing agents a simple path to alerting all stakeholders of problem-related outages. These types of notifications can be time-boxed (i.e., have an expiration) when they can be removed from dashboard widgets. Additionally, automated processes can be developed to stop alerts and notifications when an outage has been mitigated.
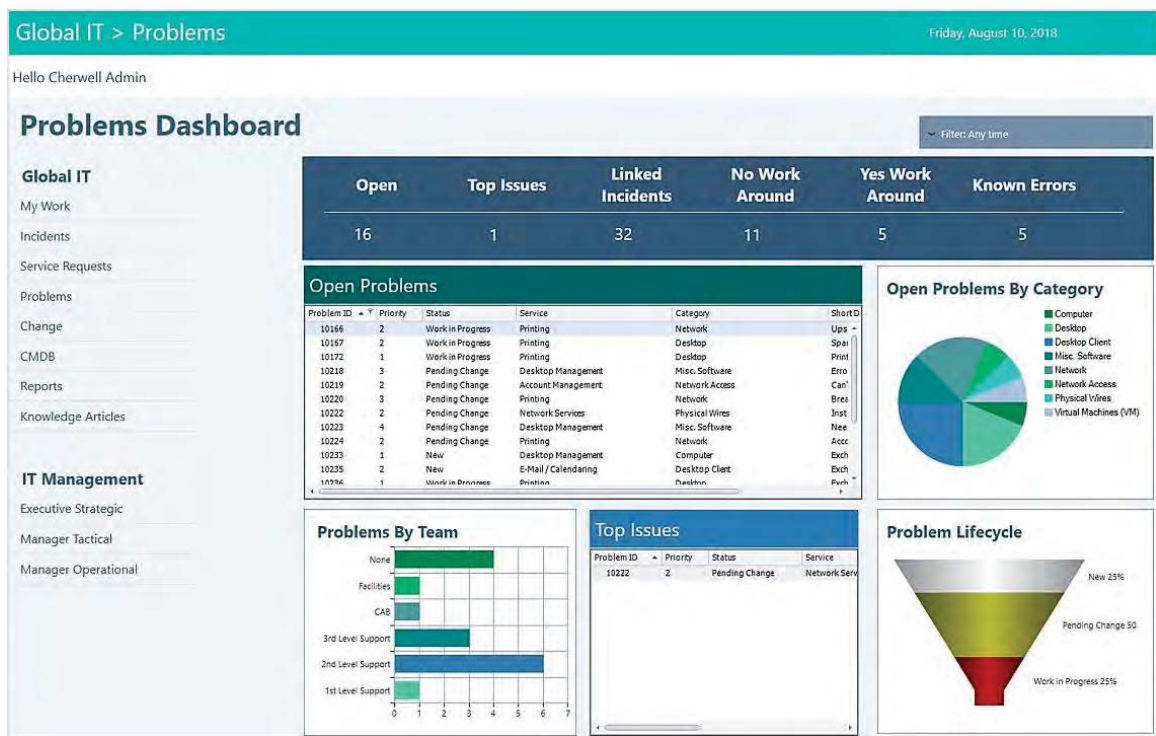
Cherwell includes the capability to search for suggested causes of problems and solutions from knowledge base records. Problems can be linked to Knowledge Articles and can be used to create such articles when a known error with a workaround, or a full solution has been implemented. Knowledge can be searched from any Problem record in the same way that Incidents and Service Requests allow for searches and consumption of Knowledge Articles.

The Problem Management module is fully integrated with the Incident Management module. A 'Create Problem from Incident' which automatically links a ticket to a new problem and populates specific fields from the Incident's data is an out-of-the-box feature in Cherwell.

Problems can be marked to be displayed in the Self-Service Portal, and the system can be configured to show such known Problems on technician dashboards as well.

Change Management

Full and formal Change Management that follows the Request for Change (RFC) lifecycle as described in ITIL is an out of the box process in Cherwell. The Airport can adopt as much or as little of this formality as is required in their environment using Cherwell's intuitive and codeless administrative toolbox.

ITIL-based visual workflows guide you through each core activity of Change Management. Know in advance how changes can impact your assets and eliminate conflicts, both up- and down-stream, with the Visualization Manager (see below). Effortlessly conduct post-change analysis to understand how changes impacted timelines, expenses, or goals with Cherwell's post-implementation questionnaire.

Cherwell has an assessment phase in Change Management that allows you to document information about risk, technical analysis, back out plans, acceptance criteria, costs items and full financial impact. These are defined out of the box, but you may add or delete criteria as needed. We have some customers in the Financial Services sector who have a much more detailed risk analysis list, for example. Any additional information can be attached to the record as well.

You define when and what assessments and information is required and when and whom is required to approve an RFC. You may also designate how many of a particular group needs to approve and on what types of changes. For example, on a Minor Change you may only require the approval of 50% of the Change Advisory Board (CAB) members, but on Significant Changes it may be 100%. Once the CAB has been notified and the appropriate percentages of CAB members have approved the RFC, it can proceed to the next step in the process. You may choose Accept, Reject, or Abstain in an approval workflow and designate when an RFC is rejected and what additional information is required when it is rejected (reason for rejection) and to whom that data needs to be sent in a notification and when through a business rule.

Cherwell will produce and display a change calendar with all upcoming changes and their scheduled dates. A Change Manager may literally move conflicting changes around through drag and drop to resolve scheduling conflicts if desired. The changes to the schedule are then propagated back to the RFC records.

As part of the change planning and implementation you may build multiple tasks, associate dependencies to define execution order and assure that all phases are complete before moving to the review and closing of the change. Post Implementation Reviews (PIRs) are built into each RFC and can be scheduled conducted at the CAB or virtually and documented in the out of the box screens for PIR. These also include the ability to create one or many PIR review questionnaires. This assures that all tasks are complete and that typical internal processes, such as a Software Development Lifecycle of Define, Design, Test, Implement, Update the CMDB and Review are completed before a change can be officially closed. And all of this can utilize templates and be modified as needed in a Cherwell "Blueprint" for recurring changes or even planned maintenance.

Service Catalog

Managing an IT organization without a Service Catalog is like running a restaurant without a menu. An effective Service Catalog provides a clear means of communicating the services offered to customers and a foundation for meaningful reporting that enables management to effectively manage. Cherwell provides an actionable, easy-to-use service catalog that presents end users with only those specific services to which they are entitled. You can even provide associated costs, estimate delivery times, and leverage product catalogs to enable charge-backs.

Knowledge Management

Reduce service desk requests by providing "Google-like" one-click access to federated knowledge searches of existing modules, PDFs, Microsoft® Office, and URLs. Cherwell's powerful knowledge management features can help your service desk team – and your customers – improve resolution times by providing a repository to successfully capture, structure, and reuse service-related knowledge.

A Pink Verified ITIL v3.0 Knowledge Management module is provided out-of-the-box at no additional charge. The Knowledge Management module includes strong metrics and approval capabilities. Cherwell's metrics allow you to run very comprehensive reports on all aspects of Knowledge Management such as usage, relevance and security levels. The Knowledge article Business Object is 100% user-definable and can be populated manually or with packaged content from any 3rd party knowledge vendor.

Cherwell utilizes what is known as a "Federated" knowledge search. Some vendors will go out and search one source, bring back those results and then go out and search another source. Cherwell will go out and search an unlimited number of sources for knowledge all at the same time and bring back comprehensive results including current or past Incidents, Problems, Changes, etc. This federated searching is available in both Cherwell Service Management as well as the Customer Self-Service Portal. Promoting Knowledge to your end users via the Self-Service portal is out-of-the box with Cherwell. Cherwell's Federated searching capabilities will also search the contents of attachments providing extremely powerful search results. Cherwell's "federated" knowledge allows that in addition to providing knowledge from the Cherwell knowledge-base, a knowledge search with return knowledge from an unlimited number and type of sources including such sources as:
- PowerPoint
- Wikis

- Intranets
- Document repositories
- Web Sources (Microsoft TechNet, Google, etc.)

You can also define the Lifecycle of a Knowledge article. Knowledge is available to both Technicians and end-users. When constructed using the native authoring tools, it is simple to use and re-use knowledge. In this case by simply clicking on the "Use" button a number of actions can happen.

The knowledge article used becomes an attachment to the record. This saves the Technician entry time. It also standardizes entries making them more comprehensible to other technicians going forward.

The form now dynamically reveals the Resolution Details Tab; which was hidden prior and automatically fills in the fields. Again, no typing was needed.

The Knowledge base is available for end-users within the Customer Self-Service Portal. This is usually a subset of the Knowledge available to IT Technicians and is managed via the applying of role-based security rules. This allows you to present knowledge to varying skill levels as needed and assure you speak to your end users "in the language of the listener" and not in "Geek-speak".

After reviewing a potential solution, the end-user can provide several responses:

- This solved my problem – which automatically opens an Incident in Cherwell, puts it in a queue, sends the user and email or anything else you would like to automate
- Populates the Incident with what knowledge the user utilized and
- Automatically Close the Incident.

The authorized purchaser will now have very powerful metrics regarding who used what knowledge, when and by whom.
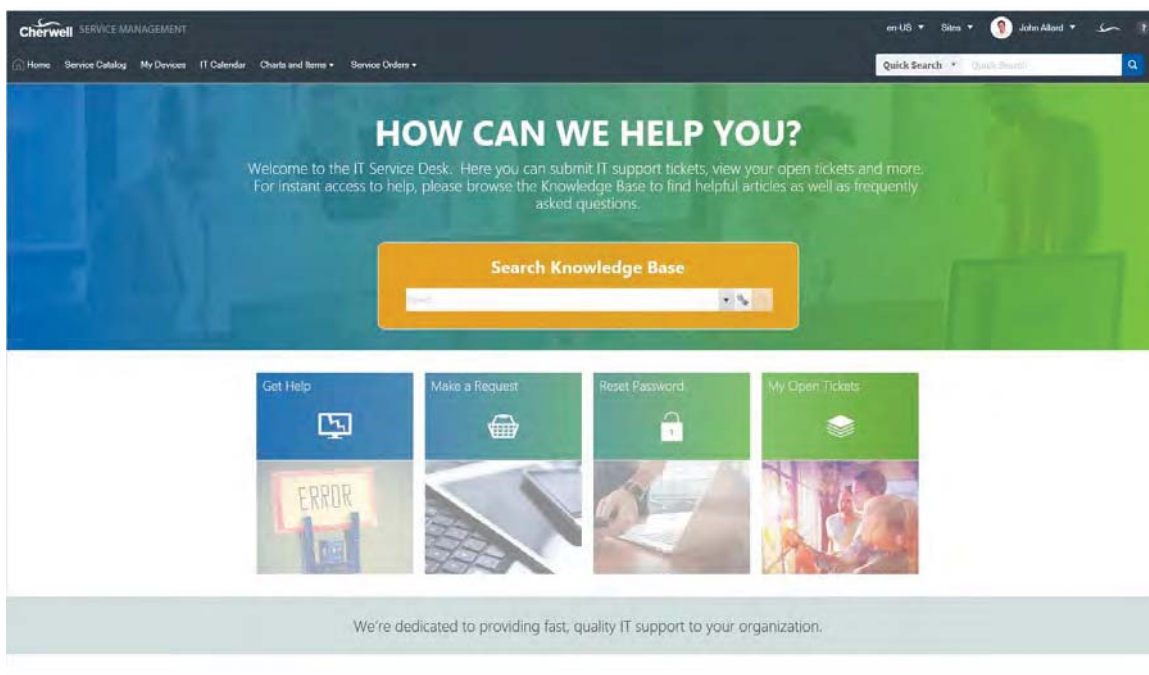
Self-Service Portal

Cherwell comes out of the box with a fully configurable Self-Service Portal that supports organizational branding, providing users with a more seamless interaction. The Cherwell Service Management's Portal Client resolves a number of common pain points and offers the following key functionality:

- Serve multiple customers, locations, constituents, etc. from one system.
- Submit and check status of their Requests avoiding calls requesting updates
- View and edit records (approvals, add comments, withdraw requests, etc.).
- Anytime, anywhere access using any modern browser, tablet, or mobile device.
- Help users to help themselves.

Cherwell's web portal is a highly interactive and user friendly. The technician interface and the self-service portal allow the user to see different information fields based on the content submitted. This provides the Airport with the flexibility to support various departments within the organization by customizing what fields are visible when users log-in and providing a responsive form that displays specific fields based on user and user input.

In the Self-Service Portal users can easily request to change assets, ownership, location, etc. and have that request routed for reviewed/approval by a support staff member. Employees can also track the progress of their request via the self-service portal.

Best of all, Airport customers using the self-service portal will never consume a license. That means as more of the Airport's end users take advantage of the portal's handy self-service, Airport technicians move beyond firefighting to become a stronger cross-functional team at no extra cost!

The Cherwell Self-Service Portal allows end-users to log in to Cherwell in a browser and create business object such as new knowledge submissions (including attachments), be kept up to date via the notes, and see a history of all business objects created. Additionally, they are able to browse the Knowledge Base, and view frequently accessed documents via the Document Repository.

End users can easily select the desired service from your provided service catalog, and track the progress of their request via the self-service portal. Technicians can quickly review, approve, and communicate to end-users the status of the request with Cherwell's simple One-Step actions. Services are defined in the Services tables and associated with any Service Level Agreements and Operating Level Agreements you define. Typically, a subset of these services is offered to end users by revealing those you want to be accessible to them in the self-service interface.

The trick is to design the portal so that it is easy and intuitive for a non-IT person to request what they need. In the self-service interface, you can provide an actionable, easy-to-use service catalog that presents end-users with only those specific services to which they are entitled. Self-Service Portal can even be configured to provide a 'shopping cart' feel to service requests, providing end users the ability to select and add various services in a single session.

As fully-configurable, wireframe software, each aspect of Cherwell Service Management can be configured to support the Airport's branding. This includes the Self-Service Portal accessed by customers and Technicians, the User Interface accessed by technicians, all email notifications, and all reports. This provides users at all levels, from executives to customers, the ability to submit incidents and consume information in a single, seamless, environment.

Branding support includes but is not limited to:

- Configuration of signature lines, fonts, content, and other sections of an email to match Airport messaging guidelines.
- Image support in all email communications, dashboards, and portals to display Airport logos.
- Customizable palettes carry Airport color schemes across all customer facing and internal views and notifications.

Dashboards and Reporting

Cherwell comes out of the box with powerful dashboard and reporting capabilities. Users will be able to run reports on any fields to which they have access.

Dashboards provide real-time, at-a-glance view to track important Business Objects and key performance indicators. Information is relevant to each User, Role, or Team vs. a generic Dashboard. Additionally, our Dashboard Viewer can allow a business manager to view a dashboard without using a Cherwell license.
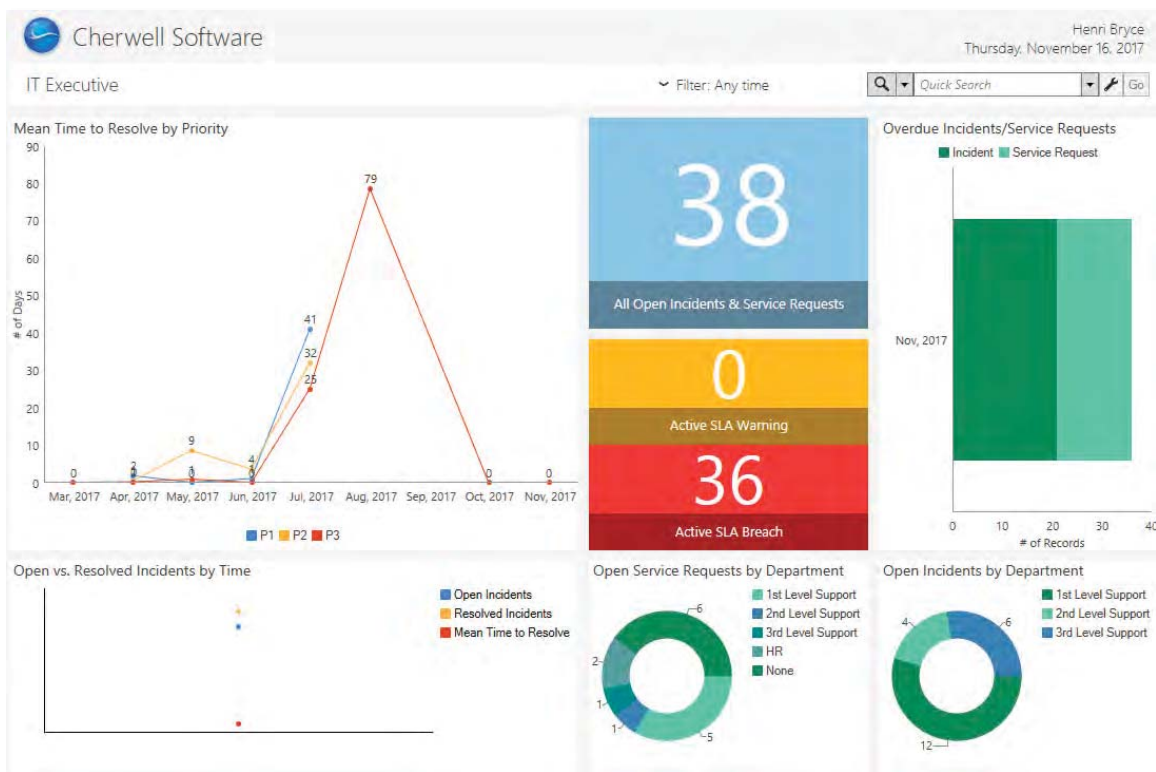
Cherwell includes a powerful built-in report writer, but also provides integrations with MSSQL Reporting Services, Crystal, and other 3rd party solutions. Our built-in report writer includes 150+ OOTB reports which can be modified and saved – or new/custom reports can easily be created using the report wizard. Every field in the Cherwell system can be reported on. The report writer interface is wizard driven, intuitive and doesn't require deep database knowledge or scripting skills to extract, transform and load data into meaningful reports that are aesthetically pleasing.

There are several file formats that reports may be exported to, including: PDF, HTML, MHT, RTF, XLS, XLSX, CSV, Text and Image. You may also schedule Cherwell reports to run and be distributed on a regular basis as needed.

Facilities Management

Cherwell's Facilities Management mergeable Applications (mApp) solution enables facilities teams to meet the needs of the business by automating workflows related to day-to-day work orders, work assignments, maintenance tasks, and facilities-related projects. With an intuitive user portal, omni-channel communication, and more, Cherwell helps modernize and optimize facilities management processes and provide a better service experience for employees.
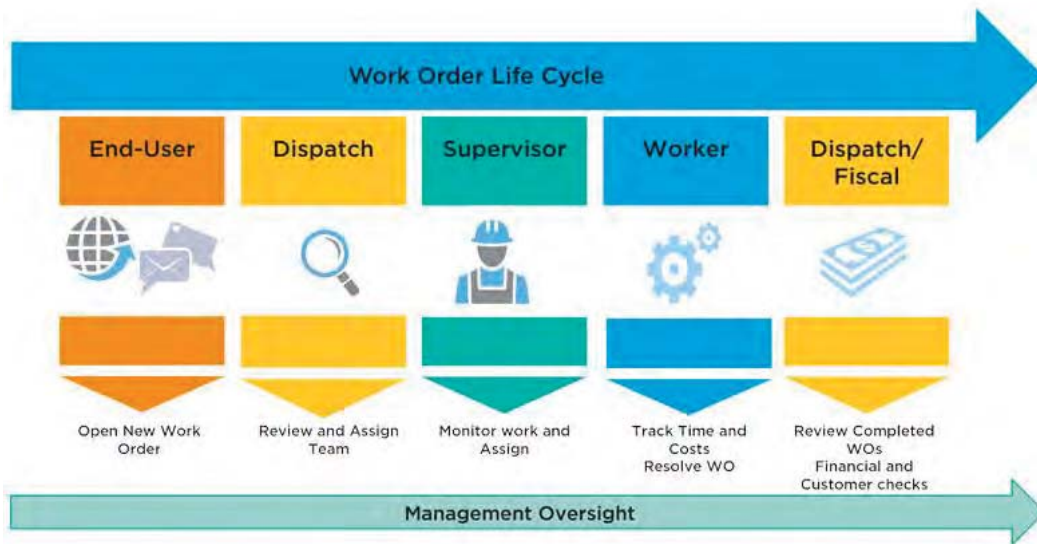
HR Case Management

Cherwell HR Case Management mApp enables organizations to streamline and automate HR service delivery for quick and efficient case management and on-boarding, along with a self-service portal for better and more productive employee service experiences.

Integrations to External Systems

Cherwell Service Management provides the tools and capabilities including a canonical REST API to integrate with business, security, discovery and inventory, infrastructure, and many other popular third-party solutions from vendors such as CA, SolarWinds, VMWare, Microsoft, SAP and Bomgar. If a prebuilt connector doesn't already exist, the customer can build integrations or Beyond20 can deliver them as a service. The Cherwell integration service provides and the maintains integrations using the Jitterbit Integration Platform Service (iPaaS) as a central hub for multiple integrations.

Cherwell integrations are "deployment-agnostic," which means you can choose on-premises, SaaS, or third-party hosting, with access to the same tools and capabilities regardless of how you choose to deploy. Cherwell integrations are also "upgrade-resilient," which means your integrations are safely protected and maintained throughout the upgrade path.

Out-of-the-Box Connectors

Cherwell Service Management includes out-of-the-box (OOTB) integrations that require only minor configurations to turn on/off, such as Microsoft Active Directory address book and authentication, Cherwell Discovery and Inventory, and Microsoft Outlook. Cherwell Service Management provides tools and functionality specifically designed to assist in configuring OOTB connector integrations.

Canonical API and Custom Integrations

Use external table imports, PowerShell, and Industry standard protocols, including Web Services (REST, JSON, XML, etc.), C#, Java, ODBC, LDAP, CSV, Excel, and SMTP to integrate with additional applications and technologies. Cherwell Service Management administrators can manually configure or create such integrations on their own or, if desired, work with Beyond20 for assistance.

Orchestration Packs

Cherwell provides orchestration packs that are a group of software "runbooks" with varying levels of configuration to meet your needs. Delivered as Cherwell mApp ("merge-able application") content via the Cherwell mApp Exchange, orchestration packs include integrations with cloud service platforms and management solutions such AWS, Microsoft Azure, and VMware vRealize. Orchestration packs also extend integrations with technologies such as Microsoft Active Directory and Microsoft Exchange.

Cherwell "Merge-able Applications" (mApps)

Cherwell mApps are a delivery mechanism for Cherwell and partner-provided integrations, extensions (e.g. surveys and enhanced process templates), orchestration packs, and line-of-business solutions for HR, Facilities, or Security teams. Additional detail regarding the HR and Facilities mApps are provided earlier in this section. These mApps are shared on the Cherwell mApp Exchange, an online marketplace where IT teams can choose from hundreds of mApps and deploy new IT and business solutions without writing code.

Cherwell provided and maintained integrations as a service delivered on the market leading Jitterbit integration platform as a service (iPaaS). Simplify maintaining multiple point-to-point integrations with thousands of potential applications.
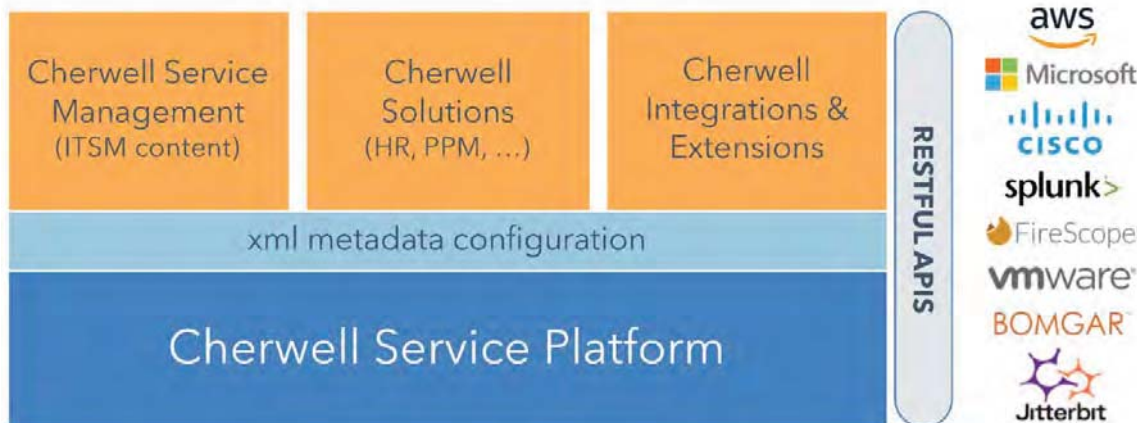
b. Alignment With Industry

Cherwell Software continues to make improvements in its service management platform through its current focus of Web UX/UI. This includes a Responsive Framework for the Customer Portal and Browser Client for the technician. Planned improvements for the Service Experience will include a mobile friendly interface, consistent dialog workflows, tab screen arrangements, editors, and limited User Admin from the Browser Client.

Cherwell has invested in performance and integrations that enable the CIO to focus on the business with a scalable and extensible platform. These improvements will include out-of-the-box integrations to "Best in Breed" products for Network management, Reporting, and Artificial Intelligence. Cherwell is also to continue to make improvements in Virtual Agents, Web Services, and API's for distributed architectures and ease of use administration, so that IT can deliver the modern service experiences their organizations expect and deserve, in a cost-effective manner.

c. ITIL Compliance Certification

Cherwell is Pink-Verified for 11 ITIL processes out of the box. The processes can all be modified to meet the Airport's unique requirements.

d. Process Modeling Technology

Ease of configuration is a key differentiator for Cherwell. The administrative interfaces are intuitive and configuration in these interfaces supports drag and drop and NEVER require you to write a script or code. Creating new fields is as simple as dropping them onto a form and labeling them. There are a wide variety of field's types available such as date/time, check box. Pick list, integer, text etc.

Cherwell's industry unique "Codeless Business Application Technology" (CBAT) which allows organizations to not only modify the existing ITIL Processes available out of the box but also provides an organization an entire Codeless Application Development Platform (ADP) in order to develop other mission-critical applications such as Facilities Mgmt., bug tracking, Project Mgmt.,

etc. and fully integrate these business objects with the other core ITIL processes. All of this is accomplished without ever writing code or scripts, and without having to utilize developer-level resources.

Graphical Workflow Editor

The graphical workflow editor pictured below makes it very easy to construct business rules and workflow unique to each process using intuitive visual configuration...again, no coding, no deep database knowledge required.

Another powerful feature of Cherwell is its "One Step" Orchestration and Run-Book-Automation actions that take workflow automation to a whole new level. Think of One-Steps as pre-programmed tasks that can be saved and re-used in future workflows or combined to completely automate a new task, such as a new hire process.

Cherwell One Steps Can:

- Create or update business objects (Incidents, Customers, Problems, etc.)
- Generate tasks
- Print
- Send e-mails
- Send Tweets
- Run reports
- Write files
- Run external programs
- Page technicians
- Excel Merge
- Queue Operations (Add, Remove, Check-out, Check-in, etc.)

There are many ways to leverage these "build-once, use again" templates across the different business objects (Incidents, Service Requests, Problems and Changes). This applies to many aspects of the solution including:

- Workflow templates such as Blueprints* and the One-Step Actions describe earlier
- the ability to nest these actions in a visual workflow for repeatable complex business processes

- the ability to pre-design templates for recurring records that pre-populate data and then use workflow templates to complete tasks
- the use of searches, reports and dashboard widgets for recurring use of the captured data.

* A Blueprint is a working copy of changes to your CSM system definitions (Business Objects, Fields, Forms, Grids, etc.) that allows you to make offline changes and then publish them to your live system at a later time.

e. Training Programs and Tools

As part of the implementation, we ask one or more of your team members to attend the Cherwell Administrator/Design course. This 5 day, hands-on, training is included and can be delivered onsite by Beyond20. This training provides the knowledge required to configure your installation, build new Business Objects, relationships and forms, and easily build and modify automated workflows within CSM. This course also provides the training for restoration and disaster recovery of CSM. Report writing and dashboard creation is also included in this training.

Beyond20 believes in a "teach-you-to-fish" approach to implementing your business solution. Our training will include a Train the Trainer process for continued training of the Airport's internal resources. This half-day to full day 'train the trainer' training session is for those who will provide users/agents training. This gives both the trainer and the end users deeper understanding of the tool and its functionality. We have been very successful providing this type of approach, and we find that most end users are ready to use the tool with minimal training. his will provide the basic tools needed for day-to-day administration of the system, including task scheduling, user imports, and other periodic administrative tasks.

As described earlier, Beyond20 offers over 350 videos covering Cherwell, including mApp creation and installation, ITSM and ITIL, and project management, and Scrum and Agile. With 15-20 new, Cherwell-specific videos added each month, this is a great way for your team to enhance their capabilities to manage and configure the CSM platform. These videos are available to the public on our YouTube Channel at www.youtube.com/Beyond20LLC.

There are Cherwell User Groups across the country, where current Cherwell users can come together and share ideas as well as discuss any issues. There is also a robust Community forum available for Cherwell users, where developers and technicians regularly collaborate to find efficient answers to questions as they arise.

Cherwel Software also offers training packages and a Video Learning Library that the Airport can leverage to quickly gain the necessary knowledge of the solution.

f. Licensing Options

Cherwell software licenses are based on a "concurrent" subscription licensing model, and all of the IT Service Management modules are included under one license. Customers who are using the self-service portal will NOT need a license. Dashboards and reports can also be viewed without consuming a license. Approvals conducted over email will also not consume a license.

Cherwell can be deployed on-premise, SaaS (in Cherwell's environment), or at a third party (e.g. Amazon Web Services, Azure, etc.). The solution is the same regardless of the deployment, so should the Airport decide to switch from SaaS to on-premise, or on-premise to a third-party, you would be able to do so with your existing licenses.

g. Experience in Partnerships and Lessons Learned

The Beyond20 Agile Service Management approach is a hybrid methodology adapted from the ITIL Continual Service Improvement Model and the core concepts of Agile and Scrum. Each project is broken into two week "sprints" with a deliverable at the end of each sprint that can potentially be delivered to customers. Each "sprint" flows naturally into the next, with no time gaps between sprints, but no single task should ever span more than one sprint.
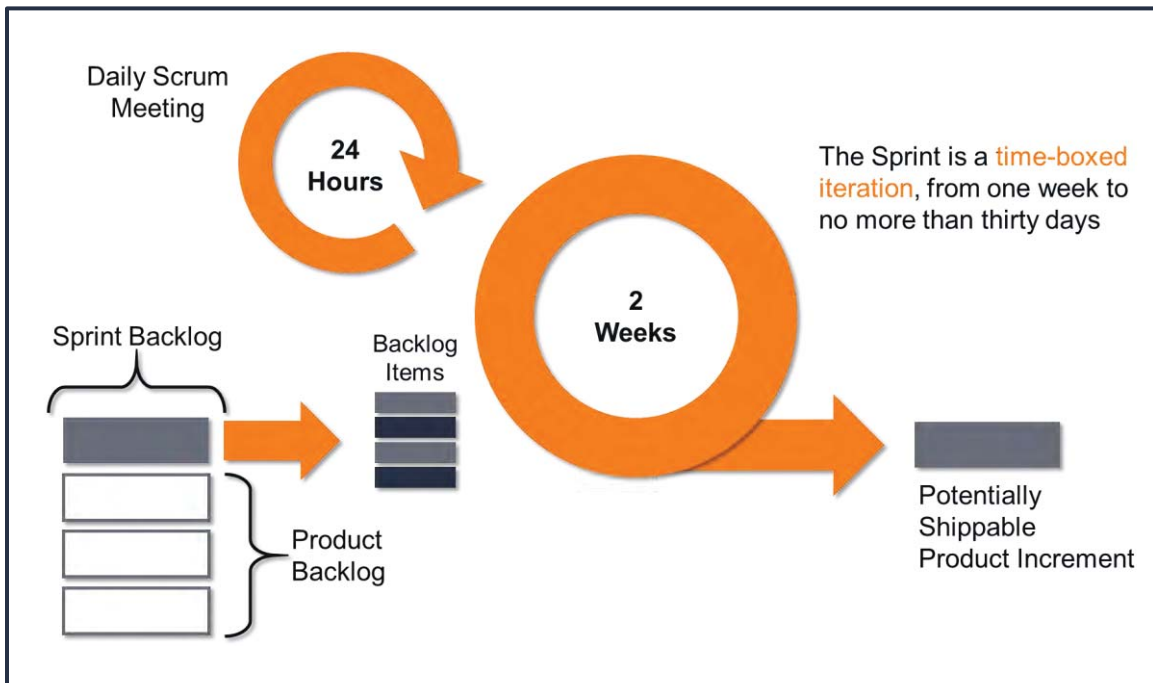
Using the approach as diagrammed above, the achievements required to complete the project are captured in the "Product Backlog" and ordered by priority. These items are then broken down into tasks that can be completed within a single sprint and assigned to the team for completion. Beyond20 team members conduct daily scrum meetings to manage the completion of individual tasks. Beyond20's Service Delivery Manager will manage the overall project using our iterative "inspect and adapt" cycle.

Using Agile project management principles will help to reduce project risk as lessons learned from previous iterations can be rapidly absorbed and applied on an ongoing basis. Each sprint will have a defined goal, with all tasks within the sprint supporting that goal. The goals of each sprint will be defined as the Beyond20 Project Manager and scrum team work through each sprint and the product backlog is prioritized. Input from stakeholders will also drive the goals and priorities of each sprint.

Tab 6) Project Approach

1. Implementation Approach

a. Describe, in detail, the approach of managing the implementation project with typical milestones. Provide an anticipated project schedule, both graphically and in text.

The scope of work requested involves the design and configuration of the Airport's Cherwell Service Management system. Design sessions will support organizational process and technical goals as they relate to the Cherwell Service Management platform. The engagement will be limited to the items outlined in the following implementation plan. Beyond20 will not perform work beyond the estimated hours without the Airport's prior, express written approval, via change order.

Note: Basic out-of-the-box (OOTB) means the CSM system, as configured after installation, with no additional configuration.

Project Management

Beyond20 Responsibilities	Customer Responsibilities
Project Kick-Off **(4 hours)** • Provide Customer with pre-installation checklist • Conduct pre-installation checklist overview session • Create the Project Plan Document • Create Project Kickoff Presentation • Plan and facilitate a project kick-off meeting with all project stake-holders at the beginning of the project **Project Management** **(52 hours)** • Provide oversight of project goals, tasks and project plan • Create and maintain Project Schedule • Facilitate periodic meetings and reviews with client and professional services teams • Provide weekly status updates to client	**Project Kick-Off** • Participate in pre-installation checklist overview session • Complete and return pre-installation checklist • Assist with the development of the Project Plan Document • Assist with creating Project Kickoff Presentation • Assist with the planning and facilitation of a project kick- off meeting with all project stake-holders at the beginning of the project **Project Management** • Participate in periodic project status reviews • Participate in the change management process as needed • Participate in the maintenance of project issues and resolutions • Attend the project closeout
Deliverables:	• Pre-installation Checklist • Project Plan Document • Project Schedule • Status Reports

Estimated Hours:	56 hours

Design

Responsibilities for workflow design and configuration activities

Responsibilities for design and configuration

Customer – Define and document in-scope processes. Work with Beyond20 to draft designs for screen layouts and forms. Define requirements and specification for reports and dashboards. Be available to provide input and make decisions on processes, form layout, etc. Provide data needed to populate tables, forms, emails, etc. Customer will define their key IT services prior to the start of the engagement in support of Incident classification. Work with Beyond20 to ensure designs are feasible and can be accomplished within the amount of time scoped.

Beyond20 – Work with Customer to design and implement Cherwell Service Management according to the Airport's documented specifications. Provide guidance to ensure the design is feasible and can be accomplished within the amount of time scoped. Beyond20 is not responsible for data modification, cleansing, or alteration before, during, or after importing data.

Beyond20 Responsibilities	Customer Responsibilities

Conduct Requirements Analysis and Solution Design Workshop
• Beyond20 will lead interactive design workshops with Airport process teams to define the CSM configuration, during which Beyond20 will review documented processes with the Airport
• Define System wide process and form standardization requirements (required data fields) to support unified reporting
• Define data capture requirements, business rules, forms, objects, searches, one-steps, security, dashboards etc., to support processes for this phase
• Review Out Of The Box (OOTB) functionality and implementation for:
    • Incident Management and Request Fulfillment
    • Problem Management
    • Change Management
    • Knowledge Management
    • Self-Service Portal
    • Dashboards and Reporting
• Determine Security Model and User Profile Screen
• Determine Priority Matrix and SLAs
• Determine Dashboard and Reporting requirements
• Determine Process integration requirements
• Discuss gaps between OOTB and desired functionality
• Determine design to be used in Cherwell
	Conduct Requirements Analysis and Solution Design Workshop
	• Ensure key stakeholders and process owners are available and engaged in the workshop
	• Come prepared with process documentation required for meaningful discussion and design for each process area
	• Determine what will be performed by Beyond20 and what will be performed by the customer
	
	Document Design
	• Assist with creation of Solution Design Document
	• Review Solution Design Document
	• Approve Solution Design Document

- Design of Request Fulfillment will consist of 3 Service request workflows
- Determine Design for Self Service Portal
- Discuss solutions and methods to achieve desired results
- Beyond20 will provide guidance to ensure the design and configuration is feasible and can be accomplished within the amount of time scoped
- Determine what work will be performed by Beyond20 and what will be performed by the customer.

Document Design
- Create Solution Design Document
- Review Solution Design Document
- Finalize Solution Design Document

Validate SOW and Design
- Reconcile Statement of Work (SOW) tasks and estimates with Design
- Create Change Order if required

Phase Specific Assumptions	- Process Design for up to 3 custom Incident/Request workflows - Form Design for up to 3 Specifics Screens - Process Design for single Portal - Email Listener and Email Templates Design - Users, Teams, and Security Design - Single Customer Type import from AD - No historical ticket imports - Activity is complete when the workshops have been conducted and the Solution Design Document has been received and approved and any required Change Orders have been approved.
Deliverables:	Beyond20 will provide the Solution Design Document detailing agreed workflows and specifications.
Estimated Hours:	64 hours (5 days of on-site design and 3 days of design document creation)

Installation and Configuration of Core Components

Beyond20 Responsibilities	Customer Responsibilities
- Confirm and validate Microsoft SQL environment - Confirm and validate Cherwell Server environment - Install*, Confirm and validate Cherwell server software - Confirm and validate Cherwell browser server software - Configure Cherwell software services* - Configure Cherwell Auto-deploy * - Test Cherwell software installation - Setup connectivity to Exchange email. - Configure Email Monitor to receive incoming e-mail to create, update, and close Incidents. - Email notification of assignment to relevant group or technician. - Email notification to customers when required. - Configure integration with Active Directory to load employee/customer table. - Configure Cherwell Users (Technicians) logins for single sign-on. - Configure scheduler for scheduled processes - Configure Auto-deploy to install client software - Set up Airport users and applicable security. Beyond20 will work with the Airport to import up to 20 system users and assign users to correct teams. - Work with the Airport to install certificates and keys in the Cherwell infrastructure and within the Airport's federated system *On-premises deployment only	- Provide access to the systems as well as technical resources familiar with each of the technologies and environments required to install and configure the core product components - Provide VPN information* - Assist with the email configuration - Provide AD/LDAP details - Provide Corporate Logo and Branding Details
Deliverables:	- Functional Test / Production Systems (two environments) - AD Integration - One (1) Email Listener (single mailbox)
Estimated Days:	16 hours

CSM Configuration

Beyond20 Responsibilities	Customer Responsibilities
Incident Management & Service Request Fulfillment **(72 hours)** • Create and Implement up to 3 Unique Specifics Forms (and supporting workflows) to support Incident Management and Request Fulfillment using configuration changes agreed to during the design workshop. • Configure Cherwell Forms, Relationships, Searches, One-steps, workflows, routing, and Business Rules according to the items agreed upon during the design sessions • Status codes and descriptions • Configure support for priority driven SLAs for Response, resolution, and escalations, including support for VIP SLAs • Perform Unit Testing	• Assign Development staff and commit their time to working with Beyond20 to implement configurations for each process area • Assign Subject Matter Experts (SME) for each integration source • Assist with Unit Testing

Variables impacting the time estimate:

• Additional Specifics to be created will impact the time estimate (Estimate assumes 3 unique specifics forms configured with up to 10 custom fields, with associated workflow. Estimate assumes 3 unique workflows configured, with associated rules and one-steps, and a total of 2 approvals (e.g. one workflow with two approvals, or two workflows with one approval each)
• Multiple (adaptive) layouts (Estimate assumes single layout per specific)

Problem Management	
Problem Management **(8 hours)** • Implement basic out of the box Problem Management with configurations identified in design sessions • Configure supporting business rules, workflow, and routing rules • Perform Unit Testing	

Variables impacting the time estimate:

- None

Change Management
(48 hours)

- Implement Change Management with configurations identified in design sessions, for Normal, Standard and Emergency changes
- Configure supporting business rules, approvals, workflows, and routing rules
- Perform Unit Testing

Variables impacting the time estimate:

- Number of approvals required in Change Management process
- Number of different change types to be configured
- Number of predefined changes with specific templates / rules
- Number of Change Advisory Board (CAB) members and whether the CAB is the same people each week or variable
- Need for post implementation reviews and/or surveys around Changes

Knowledge Management
(4 hours)

- Configure up to 5 new fields for OOTB Knowledgebase (KB) forms
- Configure 1 new KB mapping source.
- Configure default sources for Incident, Problem, and Change objects.
- Walk Customer through the OOTB Knowledge Management Workflow
- Configure approval process - OOTB
- Set to Read-Only after approval - OOTB
- Configure review process - OOTB
- Configure Knowledge Management team – OOTB
- Configure Links to the Customer's existing Knowledge sources
- Enable automation processes in support of Knowledge Management
- Perform Unit testing

Variables impacting time estimate:

- None

Self Service Portal
(24 hours)

- Import Airport Services, Categories, and Subcategories
- Configure Cherwell to support Airport classifications

- Configure system to support Incident and Service Request submission and ticket status updates via the portal for external customers.
- Configure Branding
- Configure up to two custom dashboard landing pages (logged-in and not-logged-in)
- Configure action catalog to display Service Catalog
- Perform Unit Testing

Variables impacting time estimate:

- Large/complex service catalog
- Multiple imports of service catalog data or extensive data cleanup
- Additional/complex portal configurations (multi-site, multi-tenant) will impact the time estimate (Estimate assumes 1 unique portal site)

Dashboards

(16 hours)

- Configure up to 4 dashboards as defined during the Design Sessions

Variables impacting time estimate:

- Complex reports may require additional development. If there are extensive reports needed, the number of days may need to be increased.

External Integrations

(40 hours)

- Up to 40 hours of configuration and support to establish external database connections
- Configure external database connections and scheduled job to import data into appropriate business object(s)
- Creation of business objects for importing data
- Perform unit testing

Variables impacting time estimate:

- Estimate will be largely impacted by final scope of integration (the solution to be integrated to and the business purpose is currently undefined)
- Depending on the number of external integrations required, this estimate may need to be revised.
- Integrations with external systems that require access methods not indicated above will impact the estimate
- Processing of data not accessible in standard formats (e.g., XML, JSON, relational database), with poor or inaccessible API documentation, or with bespoke configurations will impact the estimate

Deliverables:	• System configured to design document specifications
Estimated Hours	316 hours

User Acceptance Testing

Beyond20 Responsibilities	Customer Responsibilities
• Beyond20 will address UAT feedback and implement any necessary modifications to configurations based on UAT feedback and agreed specifications	• Conduct Functional Testing • Conduct System Performance Testing • Create Solution Test Cases • Conduct User Acceptance Testing • Document Defects and Enhancements
Phase Specific Assumptions	None
Deliverables:	• Modifications to configurations based on test results and agreed specifications.
Estimated Hours:	44 hours

Go-Live

Beyond20 Responsibilities	Customer Responsibilities
Go Live Support • Beyond20 will provide a "Go-Live Checklist" • To ensure successful release into production, the Airport and Beyond20 will review and complete all tasks outlined in a "Go-Live Checklist" • Beyond20 will be available for early life support of the system during the first week of system Go-Live	**Go-Live Promotion** • Promote from DEV to Production • Validate production functionality • Communicate to End Users
Phase Specific Assumptions	• Go Live Support will be provided for one "Go-Live" • System Go-Live to be completed within 4 weeks of UAT remediation completion
Deliverables:	• Go-Live Checklist
Estimated Hours:	24 Hours (12 for pre-Go-Live; 12 for post-Go-Live

Training and End-user Documentation

Beyond20 Responsibilities	Customer Responsibilities
Cherwell Administrator Training **(5 days)** • Beyond20 will provide a 5-day Cherwell Administration training for up to 10 Airport staff **Technician Training** **(8 hours)** • Beyond20 will deliver up to 8-hours in training on topics selected by the Airport for up to 16 technicians per session **Documentation and Video Creation** **(12 hours)** • Creation of Incident Management and Service Request End User guide for the Airport	**Technician Training** • Customer will deliver provider training to the technicians not able to attend the Beyond20 provided classes • Schedule training • Assign resources and commit their time to attend the provider training session
Phase Specific Assumptions:	• Technician training to be conducted in no shorter than 2-hour blocks
Deliverables:	• Up to 8 hours of technician training • Cherwell End User Guide (Incident and Service Request)
Estimated Hours:	20 hours + Cherwell Administration Training

b. Describe approach to providing quality assurance and control in accommodating the stated quality requirements.

Beyond20 will utilize the following five techniques for quality management.

Tool	Description
Scrum	Beyond20 will use the Scrum method to obtain regular customer feedback on project progress and content. Feedback will be incorporated into the Project
Bi-Weekly Sprint Reviews	Beyond20 will conduct bi-weekly sprint reviews with the Airport's core stakeholders to demonstrate development built thus far. The Airport will provide feedback which will be incorporated into development by means of the subsequent sprint cycle.
Unit Testing	Beyond20 will conduct unit testing of each requirement agreed to in the signed Design Document to ensure each unit of development (User Story) passes the agreed-upon acceptance criteria.
User Acceptance Testing	The Airport will use the agreed-upon set of requirements to conduct their own unit testing to ensure that each unit of development (User Story) is functioning as stipulated by the acceptance criteria.
RAID Log	Beyond20 will create and maintain a 'RAID Log' to track the following throughout the Cherwell project lifecycle: • Risks, Assumptions, Action Items, Issues, Decisions, Enhancements

c. Describe your recommended environments (test/dev/staging/production).

We recommend having a minimum of two environments (DEV/TEST and PROD). Cherwell provides two hosted environments with its subscription licenses.

d. Describe your transition and migration process from an existing service management solution to the Contractor-proposed solution. Detail data accuracy, data loss, and other potential issues, and state your experience at resolving such issues during previous engagements.

Beyond20 can work with the Airport to migrate necessary data over into the new Cherwell Service Management system. Typically, the tickets will not match one-to-one, so archived tickets are imported into a separate database, that the Airport will be able to refer to if necessary.

The current implementation plan does not include the migration of existing ticket

e. Describe a high-level testing strategy that defines vendor's approach to accommodating the stated testing requirements.

See below for a high-level breakdown of our testing procedure.

- Test Server startup processes
- Test IIS Application Pool access

- Test Web Services (Portal, Web Client, Forms, Auto-Deploy)
- Test User Authentication (Active Directory, local)
- Test E-mail integration
- Unit Testing
    - Process #1
        - Create record
        - Search record
        - Lifecycle
        - Notifications (E-mail)
        - Automated workflows
            - Follow User Stories
- Integration Testing
    - Integration #1
    - Test data integration (if applicable)
    - Test API connectivity (if applicable)
    - Test Scheduled Imports (if applicable)
- Load Testing
    - Client shall be responsible for Load/Stress testing of system
- User Acceptance Training
    - User Stories
        - Client will be provided with a UAT document, detailing all user stories identified during design
        - UAT results provided twice weekly until all defects have been addressed

f. Describe a high-level training strategy that defines vendor's approach to accommodating the stated training requirements.

Beyond20 believes in a "teach-you-to-fish" approach to implementing your business solution. Our training will include a Train the Trainer process for continued training of the Airport's internal resources. These 'train the trainer' training session is for those who will provide users/agents training. This gives both the trainer and the end users deeper understanding of the tool and its functionality. This will provide the basic tools needed for day-to-day administration of the system, including task scheduling, user imports, and other periodic administrative tasks.

g. Describe a high-level risk management strategy that defines vendor's approach to identifying and mitigating project risks including, but not limited to, schedule and budget variances.

Beyond20's Project Management approach follows the PMI's Project Management Body of Knowledge for best practice in Project Management. Thus, we perform risk management as follows:

- **Plan Risk Management** – performed as part of the project kick-off meeting and planning
- **Identify Risks, Perform Qualitative / Quantitative Risk Analysis, and Identify Risk Responses** – captured and communicated as part of a standard risk template (following chart)
- **Control Risks** – included in weekly project status reports

h. Describe the performance guarantees for uptime, redundancy, failover, system response times, and support response of the proposed solution.

As noted in the Cherwell Software US Hosted Environment (Appendix C), Cherwell's uptime commitment is 99.98% availability per month, except for excused outages. Cherwell's hosting operations utilize front-end/application servers that can easily be replaced as needed, leveraging the latest virtualization technologies, and redundant data connections to multiple carriers for internet connectivity.

See the Cherwell Hosting Services Addendum (Tab 3, Section 1) and Cherwell Support Guidelines (Tab 3, Section 2) for additional information.

2. Change Management Process:

a. Provide detail procedure of your firm Change Management procedure.

As noted in the Hosted Services Addendum (Tab 3, Section 2), Cherwell shall provide Maintenance of the Licensed Software as defined and set forth in the Agreement. Cherwell shall provide Customer thirty (30) days advance notice prior to applying any updates, upgrades, patches, bug fixes and new releases or versions of the Licensed Software provided as part of Maintenance (each a "Maintenance Release") to the Cherwell-hosted Licensed Software. Customer may opt out of a particular Maintenance Release, provided, however, that Customer agrees that it will not be able to decline or defer critical security patches and updates and Cherwell is free in its reasonable discretion to determine which Maintenance Releases are critical. Customer shall be responsible for applying Maintenance Releases to any locally installed portion of the Licensed Software.

All production hosted environments follow a strict change control process where the risk of any change is evaluated against the business justification to ensure a successful implementation. All change requests are reviewed to receive appropriate authorization prior to the scheduled change. This includes a two review change process and a post-implementation review. A Change Control Board manages the change process and is made up of representatives from Support, IT SaaS, and Security. The Change Control Board is chaired by the VP of IT and Security. Planned, unplanned, emergency, and exception changes to existing Cherwell SaaS infrastructure are authorized, logged, tested, and approved in accordance with industry best practices for similar systems. Updates to Cherwell infrastructure are planned in order to minimize impact on the customer and their use of the services. Cherwell will communicate with customers via email or through the Cherwell Customer Portal any time service use is likely to be adversely affected.

b. Provide sample of System Change Request Form

See Cherwell Security Whitepaper for North America (Appendix D) for additional details.

3. Escalation Structure/Plan:

a. Provide an escalation process to include list of upper management names, job titles, email address, and telephone numbers to be contacted in the event the identified issued cannot be resolved by the on-site Technician.

Beyond20 uses a tiered approach to account management to ensure effective communication at all levels. Project related communications are handled by a dedicated Project Manager, with escalation to the Service Delivery Manager, Director of Services, and Principal. Beyond20 will work with the Airport to assess the need for corrective action on any project-based deliverables, should the need arise, and will respond accordingly. Should Beyond20 be awarded the contract, contact information will be provided.

1. Detailed Pricing Breakdown

a. Year 1 Breakdown

Description	Qty.	Each	Year 1
Cherwell Service Management Subscription Licenses (billed annually) - 3-year term	20	$1,800.00	$36,000.00
CSM Annual support/maintenance	20	Included	Included
CSM Hosting Fee (SaaS Only)	1	Included	Included
Design Workshop and Document Creation	64	$243.75	$15,600.00
Implementation Services	388	$206.25	$80,025.00
Cherwell Administration Foundations	1	$14,500.00	$14,500.00
Technician Training	8	$206.25	$1,650.00
Total			$147,775.00

b. 5-Year Breakdown

Description	Qty.	Y1	Y2	Y3	Y4	Y5
Cherwell Service Management Subscription Licenses (billed annually) - 3-year term	20	$36,000.00	$36,000.00	$36,000.00	$38,160.00	$40,449.60
CSM Annual support/maintenance	20	Included	Included	Included	Included	Included
CSM Hosting Fee (SaaS Only)	1	Included	Included	Included	Included	Included
Design Workshop and Document Creation	64	$15,600.00	$0.00	$0.00	$0.00	$0.00
Implementation Services	388	$80,025.00	$4,950.00	$4,950.00	$4,950.00	$4,950.00
Cherwell Administration Foundations	1	$14,500.00	$0.00	$0.00	$0.00	$0.00
Technician Training	8	$1,650.00	$1,650.00	$1,650.00	$1,650.00	$1,650.00
Total		$147,775.00	$42,600.00	$42,600.00	$44,760.00	$47,049.60
Cumulative Total		$147,775.00	$190,375.00	$232,975.00	$277,735.00	$324,784.60

c. Terms and Delivery
See separate pricing schedule document.

Appendix A) Out of the Box Reports

- AGE Report
- Average Duration by Category
- Average Duration by Priority days
- Average Duration by Priority hours
- Average Resolution Trends
- BIOS Versions
- Category Trends
- Change Breakdown
- Change Trends
- CI Change Request Metrics
- CI Events by CI
- CI Percent Uptime
- CI Report by CI
- CI Summary Report
- Close Durations
- Closed with no Closed Date
- Computer Memory Audit
- Condensed High-Volume Customers
- Condensed Incident Duration Metrics
- Condensed Incidents with Longest Duration
- Copy of SLA Metrics of Response Time
- Cost Per Service
- CPU Speed Report
- Customer Survey Trends
- Customers and Their Incidents
- Day of Week Metrics
- Deprecate these fields
- Incident Aging
- Incident Detail Report
- Incident Duration Metrics
- Incident List with Audit Trail
- Incident List with Task Audit Trail
- Incident Volume by Source
- Incidents by Category
- Incidents by CI
- Incidents by Configuration Item
- Incidents by Owner
- Incidents by Priority
- Incidents by Source of Call
- Incidents by Subcategory
- Incidents by Team
- Incidents Resolved at First Level

- Incidents that Occur Most Often
- Incidents with Longest Duration
- Internal Customer List
- Is Description used
- Least Popular Articles
- Monthly Management Incident Review
- Most Popular Articles
- Most Used Articles
- My Closed Incidents
- My Closed Incidents by Category
- My Closed Incidents by Priority
- My Closed Incidents by Subcategory
- My Open Incidents
- My Open Incidents by Category
- My Open Incidents by Priority
- My Open Incidents by Status
- My Open Incidents by Subcategory
- My Task List
- My Teams Incidents
- Open Incidents Detail Report
- Open Problem Detail Report-Contracted
- Open Problem Detail Report-Expanded
- OS Report
- Overdue Incidents
- Overdue Purchas Orders
- Overdue Sales Tasks
- Past Month Average Duration by Category
- Past Month Average Duration by Priority
- Past Month Average Resolution Trends
- Past Month Day of Week Metrics
- Past Month Incident Duration Metrics
- Past Month Incidents by Category
- Past Month Incidents by Owner
- Past Month Incidents by Priority
- Past Month Incidents by Subcategory
- Past Month Incidents by Team
- Past Month Incidents Resolved at First Level
- Past Month Incidents that Occur Most Often

- Past Month Incidents with Longest Duration
- Past Month Staff Workloads
- Past Month Top 10 Customer Activity
- Past Month Top 10 High Volume Customers
- Past Month Trends by Day
- Past Month Trends by Week
- Past Week Average Duration by Category
- Past Week Average Duration by Priority
- Past Week Average Resolution Trends
- Past Week Incidents by Category
- Past Week Incidents by Owner
- Past Week Incidents by Priority
- Past Week Incidents by Subcategory
- Past Week Incidents by Team
- Past Week Incidents that Occur Most Often
- Past Week Incidents with Longest Duration
- Past Week SLA Metrics of Resolution Time
- Past Week SLA Metrics of Response Time
- Past Week Staff Workloads
- Past Week Trends by Day
- Past Year Average Duration by Category
- Past Year Average Duration by Priority
- Past Year Average Resolution Trends
- Past Year Category Trends
- Past Year Change Breakdown
- Past Year Change Trends
- Past Year Day of Week Metrics
- Past Year Incident Duration Metrics
- Past Year Incidents by Owner
- Past Year Incidents by Team
- Past Year Incidents Resolved at First Level
- Past Year Service Trends
- Past Year Staff Workloads
- Past Year Top 10 Customer Activity
- Past Year Top 10 High Volume Customers
- Past Year Trends by Week
- Planned Changes
- Post Implementation Review
- Proactive Service Changes
- Proactive Service Problems
- Problem Detail Report
- Problem Impact Metrics
- Problem Metrics
- Problem Report
- Problem Summary
- Problem Summary Report
- Problem Trends
- Problems by Category
- Problems by Impact
- Problems by Service
- Problems by Status
- Problems Linked with Incidents
- Report Name
- Service Desk Overdue Incidents
- Service Trends
- SLA Metrics of Resolution Time
- SLA Metrics of Response Time
- Software Summary
- Staff Workloads
- Status of Purchase Orders
- Surveys with Overall Score
- Task Metrics
- Team Customer Survey Results
- Technician Customer Survey Results
- Top 10 Customer Activity
- Top 10 High Volume Customers
- Top 10 Problems
- Top 10 Problems by Category
- Top 10 Problems by Team
- Top 10 Problems old
- Trends by Day
- Trends by Week
- Unsatisfied Customer Incidents
- Vendor Grouping
- Weekly Management Incident Review
- All the Incidents Associated with Each Problem

Appendix B) Cherwell Application Security Whitepaper

See following pages for Beyond20's Cherwell Application Security Whitepaper.

CHERWELL SERVICE MANAGEMENT APPLICATION SECURITY

PREPARED BY:

Mark D. Hillyard
SENIOR SOLUTIONS CONSULTANT

Table of Contents

Cherwell Service Management
Application Security
Navigating Multi-Tiered Security

1   Background

Cherwell Service Management (CSM) was created with highly configurable security front and center, and it has been a cornerstone of the platform in every release. However, because of its granular and flexible design, the security features can present a labyrinthine challenge to new administrators. This guide is intended to demystify this key element to configuration and give all Cherwell Administrators (new and experienced) confidence when securing the CSM platform.

2   Overview

CSM was designed with a four-tiered security model. Though the lowest tier (user) is seldom used to apply security, it is possible for use cases where this is desirable or necessary.

The platform comes standard with several Security Groups (Tier 1), Roles (Tier 2), Teams and Workgroups (Tier 3), and users (Tier 4). As a best practice, always duplicate the existing Security Groups to create new ones. Find the Security Group closest to the level of security required, and copy it as a template to be modified. Often, the existing Security Groups will be sufficient for a new system, and it is always recommended that the system have the smallest number of Security Groups possible to provide the appropriate diversity of security rules.

Along with the various tiers, there are two primary aspects of security: Rights (what a user can do in the system), and Business Objects (what a user can do with records within the system). Each is very distinctive and provides administrators a wealth of options with regard to security. As a part of the system design process, it is important that an implementer provide a detailed guide to CSM administrators, so that they can both familiarize themselves with the structure of system security and provide feedback as to any changes or enhancements that need to be made prior to releasing the system to end users. This also empowers the administrators to make key decisions as to how their system should operate, and who should have access.

The third pillar of the Cherwell security model defines how users will access the system. Because there are two distinct types of users in any ITSM tool, it is important to distinguish each as it relates to access and security. The first type of user is what CSM refers to as a Licensed user. These are the analysts, technicians, admins and any other individual that may need to access the client (either using the standalone smart client or the browser-based client tool). These users will consume a license each time they log in, and

they will maintain that license until they log out or are disconnected by an idle timeout. Security for this type of user is extremely important, as each individual will have access to create, modify and, in some cases, even delete records. If an administrator provides too much access, the system can be damaged; however, if too little access is granted, users will be unable to perform their assigned job function. Providing appropriate security to Licensed users not only protects the CSM platform, but it is also a key ingredient to user buy-in. The other type of user is what Cherwell terms a Customer. This can be, and often is, misinterpreted as being an external user that is not employed by the organization. While this is one possible scenario, in the CSM platform, a Customer is defined as any unlicensed user that can submit service requests, incidents, and sometimes other types of records, such as change requests, problems, or even knowledge articles. This type of user, however, has very little system access. Because they are unlicensed, they are unable to modify any record where they are not considered the 'requester' (this is a unique database attribute that is set within the business object properties, and it can be configured for any business object that might be exposed to unlicensed users). Additionally, these users can only access the system through e-mail or the self-service portal. Because of this restriction, many security settings are completely unavailable to these users and are not necessary to configure.

Finally, there are several areas of the CSM platform that can be bundled into what could be defined as Security Accessories. Included here is authentication method—Cherwell supports standalone user authentication, LDAP authentication (including Active Directory integration), and SAML authentication (including Active Directory Federated Services (ADFS)). Active Directory (AD) authentication is still the most popular method of user access, but SAML is becoming more and more popular as companies shift their internal authentication methods to SaaS solutions, such as Microsoft® Azure. Also included are file attachment settings, which govern the size and types of attachments that can be stored in the system, and REST API client settings, which are required when configuring API-based integrations with third party tools like JIRA Software. Lastly, there is a relatively new but powerful security accessory, and that is ability to encrypt data at the field level. Not only can the data be encrypted, decryption can be controlled by the existing security structure, so it is very simple to grant/revoke access to users, as required.

3   Security Model

As described in the overview, the Cherwell Security Model is made up of four (4) distinct tiers, or levels, of security. The interactions of these different tiers is very important, and it all begins with the user (Tier 4). Every user in Cherwell is assigned to a single Security Group (Tier 1). A user may not be a member of more than one Security Group but must be a member of one Security Group. Within each Security Group, there are one or more Roles (Tier 2). Each user that is assigned to a specific Security Group has access to any Role that is a part of that Security Group. Each user can be assigned to zero or more Teams (Tier 3) *(see Figure 1)*. It is not advisable to have a human user (one that is used by an individual to log into the system and perform work) that is not assigned to at least one Team. Once a user is assigned to one Team, a default Team must be chosen.
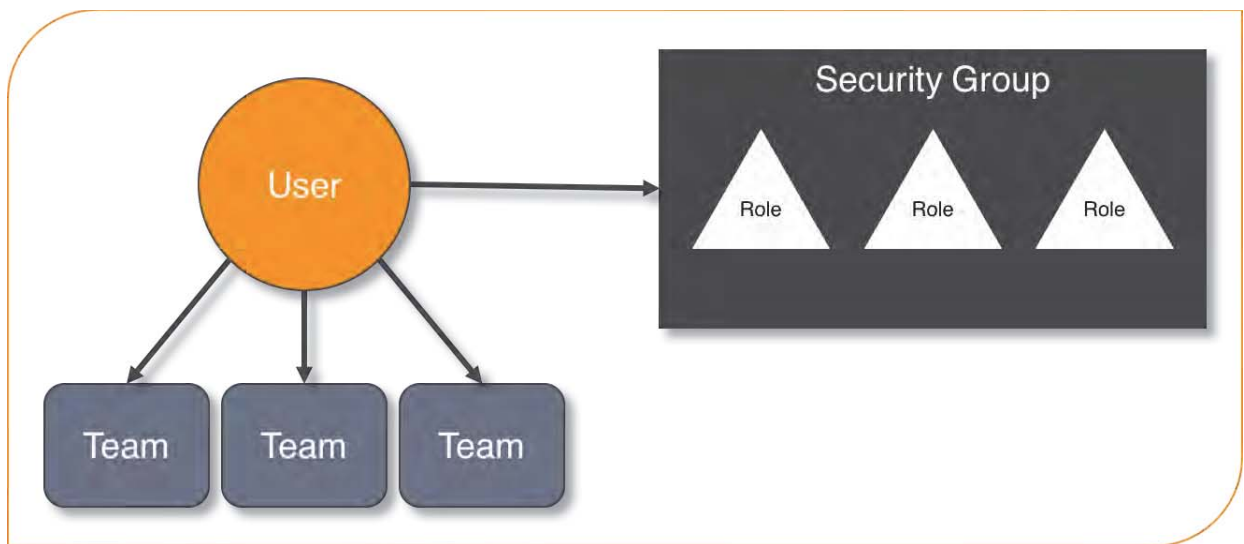
Figure 1

When a user logs into the Cherwell Client, he/she is prompted for the Role to use (if more than one is available in the user's Security Group). This Role will be used throughout the user's session. While logged in, a user has access to all of the Teams that he/she is assigned in the system. These concepts will be further defined in the sections below.

3.1 Tier 1 – Security Groups

3.1.1 Purpose

The Security Group is the keystone for all Cherwell activity. Each distinct group controls nearly every aspect of what can and cannot be done within the platform. This includes things as basic as whether a user has access to the Client (Smart or Browser) to extremely granular things such as visibility and/or edit rights to a single field on a form, and everything in between.

3.1.2 Best Practice

As previously discussed, it is considered best practice to keep the number of Security Groups in a single Cherwell implementation to a minimum. Unless there is a compelling reason to have several Security Groups with only minor variations in access, such as regulatory requirements or an overly curious user base, having many Security Groups only adds to administrative overhead, and it can lead to costly mistakes when updating access across several Security Groups at once. Where possible, it is advisable to train users where the lines are drawn as far as system access goes, and in those cases where two similar groups exist with only slight variations in access, provide full disclosure to each group and explain that while they each have access to certain aspects of the system, only one group should ever make changes in that manner. If the nuance in access is expressly around record and/or field visibility, this can be handled through other means

at a lower Security Tier, negating the need to create entirely new Security Groups for this purpose.

3.1.3 Configuration

This is not to say that an administrator should not create a new Security Group when it makes good sense to do so. In fact, it can be of great benefit to split out functions into multiple Security Groups. For example, if CSM is being used to perform multiple functions within the organization, such as Human Resources (HR) or Facilities management, there is a compelling argument for creating individual Security Groups for these functions. Often, especially as it relates to HR, some records should be completely hidden from other groups (think of termination requests). In this instance, it is likely imperative that such records do not appear in searches by non-HR groups. When configuring other non-IT functions within the CSM platform, such as Facilities, it may be more convenient for those groups not to see IT related records, and in this case, creating a Security Group specifically for them gives the administrator the ability to hide unrelated records, and even processes, simplifying the user experience for non-IT functions *(see Figure 2)*.
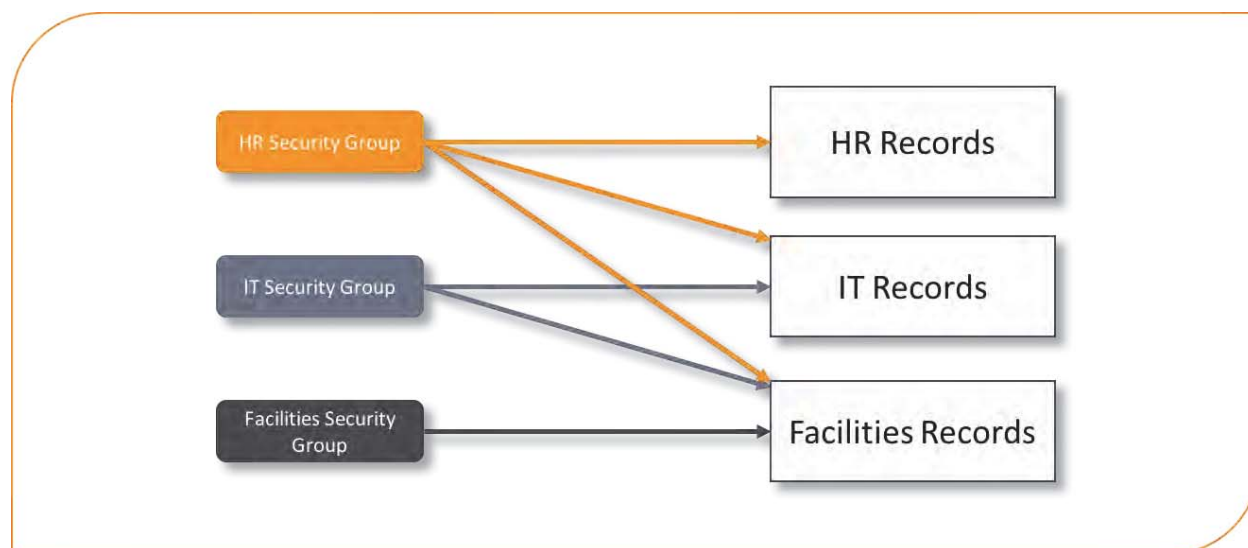
Figure 2

In this example, the HR Security Group has access to any record in the system. The IT Security Group has access to IT Records and Facilities Records, and the Facilities Group only has access to Facilities Records. The constraint on HR records is one of necessity, as there are always HR related issues that must be restricted to only the HR function. The constraint for the Facilities Security Group is one of convenience. There is generally no reason that a user performing the Facilities function would need access to IT Records, so the administrator can limit the records available to provide a simpler, cleaner user experience for Facilities. It might also be advisable to limit HR access to other types of records for the same reason, or it may be that all records should be visible to HR. That is a decision left to the administrator and the platform stakeholders. But this illustrates the

flexibility of the platform as it relates to access and user experience. It is important to note that if a set of records is made unavailable to a Security Group, that group will not even be aware that those records exist in the system. They will be removed from search results, dashboards, related item tabs and controls, etc. Exceptions can be granted based on specific criteria (such as Task ownership, which is a common request from administrators), so that in very specific cases, one or more of these records can be exposed to a different Security Group for action or disposal.

Beyond record visibility and access, Security Groups also control all Rights access within the platform. These are things like the ability to modify Dashboards, Reports, Calendars, etc. As well as whether or not a user can launch the Client (Smart or Browser) and/or the Administrator application. There are, in fact, hundreds of individual Rights that can be granted or denied for each Security Group. For the most part, these Rights are configured for non-administrative accounts (Administrators generally are given all Rights within the system); however, it can be useful to create tiered Rights in larger implementations where there may be value in creating sub-administrators or junior administrators. In these cases, some higher level Rights may be granted to a junior administrator without giving away the farm. For instance, a junior administrator may be given the right to access the Administrator tool, but he/she may not be able to publish a blueprint, reserving that Right to administrators only.

3.1.4 Summary
- Security Groups control all access to the system, Business Objects, and Rights;
- It is best practice to limit the total number of Security Groups for ease of administration;
- Security Groups can be used to limit access to certain records within the system;
- Security Groups are used to control specific access Rights throughout the platform.

3.2 Tier 2 – Roles

3.2.1 Purpose
Roles occupy a unique position within the Security model in that they are not assigned to users, and users cannot be assigned to specific Roles. Instead, Roles are assigned to Security Groups—sometimes to more than one. Once a Role is assigned to a Security Group, all members of that Security Group have access to log in under the Role.

3.2.2 Best Practice
Roles are best used when controlling user experience in CSM. Most commonly, Roles are responsible for providing default dashboards, heads-up display, task pane, and Business Object visibility. This is a convenient way for administrators to control how each different type of user interacts with CSM.

Roles are also one of the more underutilized functions in CSM. In most implementations, only two major applications of Role are leveraged by the system: the first, and most

common, is utilizing Roles for self-service portal users, differentiating this view from the default, Client view—this is a built in feature, and most administrators do not make any major modifications; the other is to control the default dashboard experience for various users in the Client view. However, there are quite a few additional uses for Roles, and these can be very useful, especially for implementations with multiple user types (e.g., IT, HR, and Facilities each requiring different access, but also a different user interface).

3.2.3 Configuration

Common configuration of Roles is very straightforward within CSM. Within the administration tool, each Role can be configured separately, providing the ability to select custom default dashboards, task pane items, and even setting what business objects are available for search and creation. Keep in mind that Role selection does not specifically alter the level of access a user has within the tool, save for very specific instances, when a Role may be used to limit access to a field, link or One-Step within a Business Object.

Limiting functionality based on Role is not a common practice, but it does have some valuable use cases. One of the most common uses is to restrict the ability to step through a workflow based on Role selection. For instance, when dealing with Knowledge Management, the organization may wish to limit which user(s) can publish an article. This could be limited by Security Group, but often this does not work out, since each user with this authority may have varying access requirements based on their normal function within CSM. In this case, a Role could be created for this specific purpose—Knowledge Management. If one of the users assigned to a Security Group that contains this Role logs in using the Knowledge Management Role, the user would then have access to publish a knowledge article. The same user, logged in with a different Role, would not have this authority *(See Figure 3).*
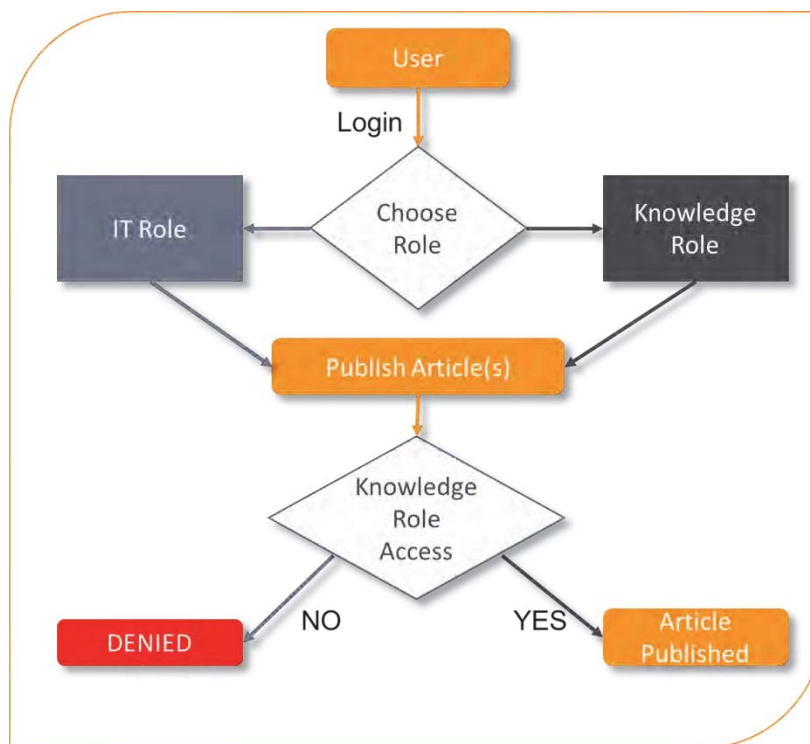

Figure 3

As demonstrated in the previous section, access to records can be limited based on Security Group membership, but one can also control the overall user experience based

on Role usage. Take, for example, the requirement that Facilities users need to have a different set of fields and a different workflow when submitting a Service Request. In this instance, the Administrator could use a Specifics form to provide additional fields necessary to fulfill such a requirement; however, all of the existing fields on a Service Request form may not be necessary, or even well understood, within this context. In such a case, an entirely different form can be presented to the Facilities Role with different requirements and a different workflow (*See Figure 4).*
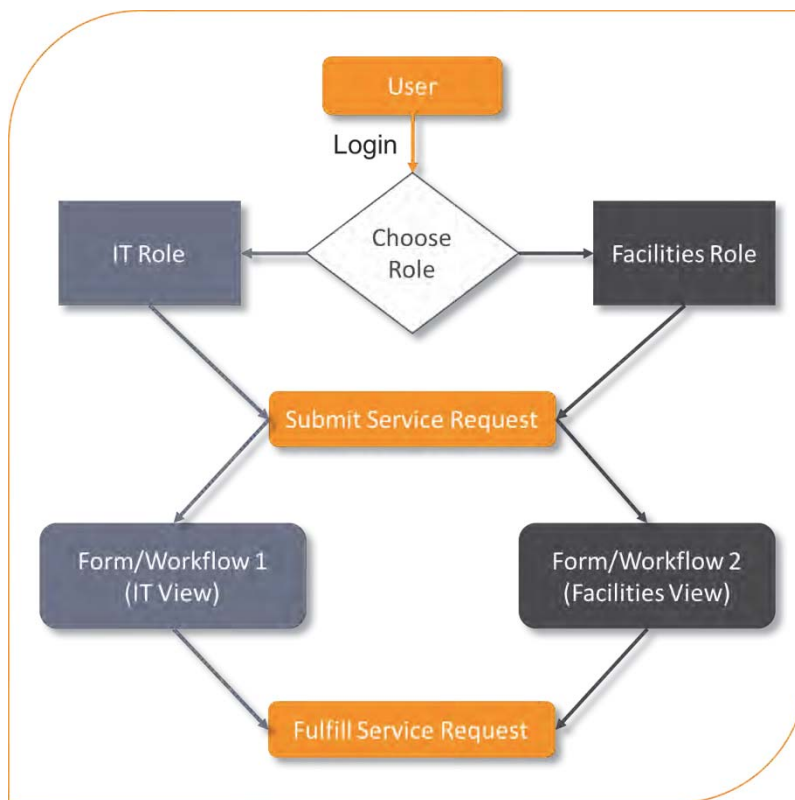
Figure 4

As you can see, the same user may login with two different Roles, and each allows the user to submit a Service Request in CSM; however, based on the Role selected, a different form and workflow will be followed. Once the work is completed, CSM can be configured to resolve the Service Request and provide a seamless experience to the original end user.

This configuration may be more complex than is often required, but it can be extremely useful if widely varying requirements exist for different Roles. It is also important to note that when adding a Business object to a new Role based view, forms and fields are no longer aligned. This means that if a particular field needs to have the same functionality across more than one view, the updated attribute(s) must be applied to each view individually. This can lead to more complicated administration and higher rates of inconsistency across views. Whenever an Administrator determines that a separate view is necessary for a specific Business Object, it is critical that detailed documentation is kept current for the system, especially if more than one Administrator is responsible for system upkeep.

Finally, keep in mind that if a new view is created, it is not necessary to copy Business Objects to the new view if they do not need to be unique. For example, while Incidents and Service Requests may need different forms and workflows for IT and Facilities, both Roles may interact with Knowledge Management identically; consequently, the Administrator would not create a copy of Knowledge in the new view. In this case, CSM

will simply utilize the same forms and workflows from the default view. This can simplify things considerably, allowing the system to continue to use pre-existing configurations when a custom view is not required.

3.2.4 Summary

- Roles are assigned to Security Groups, providing access to all users in the group;
- Roles can be used to provide a different user experience;
- Roles can restrict access to certain workflows, links and one-steps;
- Creating multiple views requires rigorous documentation and change processes to ensure consistency across the tool.

3.3   Tier 3 – Teams and Workgroups

3.3.1 Purpose

Teams and Workgroups are meant to provide functional structure for users and customers within CSM. While there is little security that can be provided by Team or Workgroup membership, this is a key tier to the overall Security Model. A User can be assigned to zero or more Teams within CSM; however, it is important to remember that if a User is a member of at least one Team, he/she must be assigned a 'Default Team'. This definition is used for several One-Steps within CSM, and the system will not allow a User who is assigned to a Team to be saved without setting the Default Team membership for that User.

3.3.2 Best Practice

All human Users should be assigned to at least one Team within CSM. The only Users that should exist without Team membership are service accounts, such as the default administrator account, and any accounts set up to run the various Cherwell Servers (E-mail Monitor, Scheduling Agent, etc.). This can also be used for any User that you do not want to be assigned (or own) any record in Cherwell. It is possible that some members of the organizational leadership may never need to work with records in CSM, but they may need access to the Dashboard Viewer application. This type of User should not be added to any Teams, so that records are not assigned to him/her mistakenly.

Within CSM, there should be as many Teams as there are functions. What this means is that if you have Facilities Users disposing of Service Requests, there really should be a Facilities Team. But there may be several Facilities related Teams as well. Perhaps there is a specific function for setting up conference rooms, and a different function for deploying cubicle furniture for new employees. This might require two separate Teams in CSM to ensure Requests and Tasks are appropriately assigned.

Because it is possible to assign Users to multiple Teams in Cherwell, it is important that Administrators maintain this Team membership rigorously. It can become very messy if a User transfers from the DBA Team to the Web Development Team and no changes are made to his/her Team in CSM. In such a case, the User would be inundated with

database requests and incidents but receive no notifications regarding web application bugs, etc. Additionally, it may be useful for an Administrator to assign himself/herself to many of the Teams in CSM while testing, but this can become very burdensome during normal daily operations. Users should only be assigned to the Teams for which they regularly perform functions.

As mentioned, Teams allow for some limited security within CSM, and it is possible to restrict access to records and fields based on team membership and status (fields and records can be constrained to just managers of a team).

3.3.3 Configuration

Configuring Teams is very simple in the Cherwell Administrator application. Each Team is added individually, and users can be added from the Team administration window, or a single user can be added to many Teams from the User Info administration window. When adding from the User Info interface, it is possible to flag a user as a Team Manager. This information is used for Security purposes when limiting access to specific records and/or fields within a Business Object. Any User can be the manager of multiple Teams, and each Team can have multiple Managers. This can get problematic if you are using Team Manager for any other purpose in the system, and using the Team Manager flag requires specific external data views to access—this functionality is outside the scope of this paper.

Once a Team is added and has Users and at least one manager associated, it can then be used to constrain certain objects and fields based on Team membership and status.
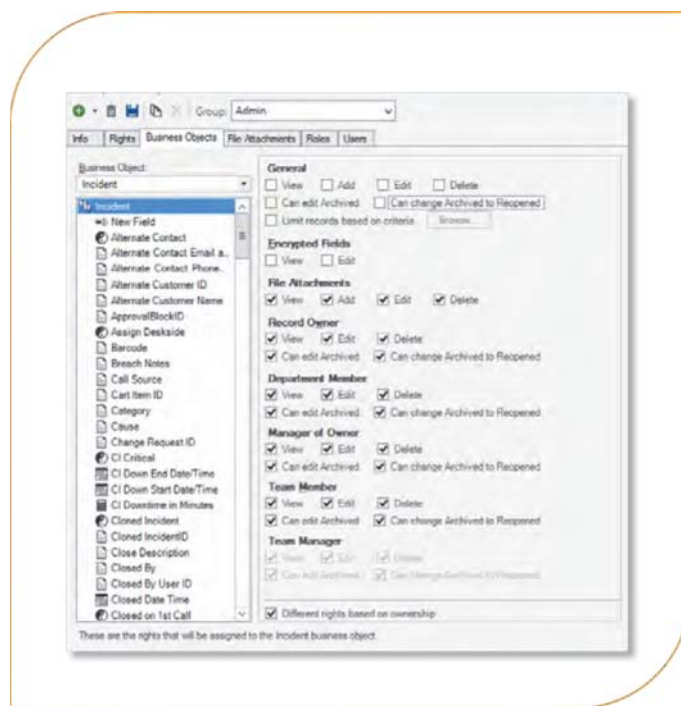

Figure 5

Utilizing the Security Group management tool within the Administrator application, entire Business Objects, as well as any individual field, can be configured to allow access based on Team membership (see Figure 5).

As you can see, there are a lot of extended options that can be controlled based on the ownership of a record. You will also notice that there is a Department membership section as well. This is a very handy additional field available at the User level that can be used to further control access. This level of granular control is available at the field level as well.

Another way to use Team membership to control access to records—especially in those cases where certain types of records should be completely hidden from various Teams in the system—is to utilize a custom expression to limit visibility. Such an expression can be built to explicitly allow access to records based on various criteria (ownership, classification, etc.) and then limited by Team membership. As can be seen in Figure 5, there is a checkbox to limit availability based on an expression. This gives an Administrator the ability to write any expression to control access to a Business Object.

3.3.4 Summary

- Teams and Workgroups contain Users and are not constrained by Security Group or Role;
- A User can be assigned to zero or more Teams;
- Once a User is assigned to at least one Team, that user must have a Default Team assignment;
- Service Accounts and Administrator Accounts should not be assigned to any Team;
- Each Team can have zero or more Managers;
- Team membership and status can be used to constrain access to Business Objects and/or fields;
- Custom expressions can be used to restrict visibility of certain Business Objects

3.4 Tier 4 – Users

3.4.1 Purpose

Users are the core unit in Cherwell. Each individual User is assigned to a single Security Group, can access any Role contained within that Security Group, and can be assigned to one or more Teams in the system. Each of these levels, as discussed, can provide varying degrees of security. It is important to note that there are two distinct User types in Cherwell: Licensed Users—commonly referred to as Technicians, and Portal Users—generally known as Customers. These will be discussed in greater detail later on, but it is important to understand that Technicians generally have both a Licensed User account as a Portal User account. While they will almost always have the same credentials, they are used for very different purposes. While a Licensed User has the ability to log into the Cherwell client application and modify any ticket for which they have been given rights, Portal Users can only log into the self-service portal and work with tickets they have submitted to the system. This is a very critical point to fully understand. It is quite common to forget that when a User logs into the self-service portal, his/her rights are much more limited than if he/she logs into the client application. It is, in fact, a different User account that is being used to access the self-service portal.

3.4.2 Best Practice

There has been much discussion around how to best allocate Users in the system, specifically regarding Licensed Users. The main point of contention revolves around

Administrator level Users. Some organizations choose to provide a single User account for each Administrator, which effectively gives that User an additional level of security access even when he/she is simply working on a record in the system as a Technician. The flip side of this philosophy is to create Administrator specific accounts for each Technician that is designated as an Administrator for the system. This approach splits the access—even if only administratively—for that User, ensuring that when he/she is working on a record, the access level remains the same as any other non-Administrator User in the system.

The fact is, either method works, as long as the appropriate policies and training are provided to ensure that the chosen process works as intended. This paper recommends utilizing separate accounts for system administration and daily work. Such separation provides a greater deal of flexibility from a security standpoint, and it ensures that users that have Administrator accounts are not accidentally performing restricted activities in the course of their normal daily tasks. If this path is chosen, it is important to ensure that the Administrator account created for each of the system's administrators does not get assigned to a Team to ensure that no Incidents and/or requests are assigned to that User. Instead, daily work should be assigned to the support team/individual responsible for disposing of that type of Incident/Request.

Since the majority of Users are usually being imported from an external authentication system (such as Microsoft® Active Directory), a good amount of data will be automatically mapped into the UserInfo table (this is the table in Cherwell where Licensed User data is stored). Common fields not included in an import are Department (which can be useful as a security tool, as explained below), Phone Numbers, Address, and Physical Location (such as an office or cubicle designation). If it is important to your organization that these data points are captured, it will require modifying the default data mapping included with CSM. This is similar for Portal Users, as some fields may not be mapped by default.

User Departments can be extremely helpful as an additional security parameter for Licensed Users. Each User can be assigned to one Department in the system, and this can then be used in controlling access to Business Objects and fields (see Figure 5). If Department is an attribute in the LDAP system being used for authentication, this can be mapped directly to a User record in CSM.

Portal Users are nearly always imported from an external source, whether it is a system such as Microsoft® Active Directory or a flat text file. As most systems will have hundreds, and often many thousand, Portal Users, it is considered overly cumbersome to attempt to populate this table manually. There are occasions, however, when the Cherwell table must be maintained using flat text files, instead of direct data imports/links. In these cases, it is necessary to build a temporary table to hold the periodic import of updated user information, and then either a SQL stored expression, or a Cherwell One-Step must be utilized on a scheduled basis to update the Cherwell Customer table. The reason for this is that the import of a flat-text file is not considered 'intelligent'. That is to say, the

only options for importing flat-text into Cherwell is to either augment the existing data with newly created records or to completely replace the records already in the table. Neither of these is a viable solution for the following reasons: 1) if the import only creates new records, then the existing data will never be updated, and you will be left with stale information; 2) if the import replaces the data already in the system, new unique identifiers (known as RecID's) will be created, thus leaving relationships between Users and their records broken—the system will be filled with 'orphaned' records with no requester associated. So, the alternative is to create a temporary table to hold all of the newly acquired data, and then run a script (either in SQL as a Stored Procedure, or in Cherwell as a One-Step) to update the existing data in the Customer Business Object. The specific process for how to write this script is outside the scope of this paper.

3.4.3 Configuration

Licensed Users (Technicians)
These Users are configured using the Administrator application. They can be imported (from a supported LDAP system), or they can be manually added by an Administrator. Regardless of how Technicians are added, they must be created one at a time. There is currently no way to mass import Licensed Users into Cherwell. When imported, Security Group membership is selected prior to creation of the User record. It is important to pay attention to this fact, as users can be imported using the wrong Security Group, and that can cause issues—especially if a User is erroneously imported into a Security Group much higher than one to which he/she should have access. Users can be imported from multiple sources, so it is not necessary to only import from a single LDAP source (or even a single domain, in the case of Microsoft® Active Directory). This can be helpful in highly complex systems where multiple authentication sources may be in use. For imported Users, authentication is handled by the source system, so there is no need to add a password for these records. For manual entry, a username and password must be provided. The only requirements at creation for any User (whether imported or manually added) are a username (and password for manual entries), and a Full Name. It is, however, very important to also include contact information—an e-mail address at the very least. Team membership can wait until all Users have been added to the system.

Once a Licensed User has been added to the system, he/she will have immediate access and rights as assigned for his/her Security Group. There is no waiting period or need to reload data definitions for the creation of a new User.

Security Group Mapping
If the organization is using Active Directory, it is possible to map AD Groups to Cherwell Security Groups. What this allows an Administrator to do is provide a way for Licensed Users to be auto-created upon login. Essentially, by mapping an AD Group directly to a Cherwell Security Group, when a member of that AD Group logs into Cherwell for the first time, his/her User will be instantly created in the system, mapping all selected fields to his/her User record. However, this does not add the User to any Teams in Cherwell. This is a key point, since without Team membership much functionality may be limited. Team

membership is always a manual process in the Cherwell system. This is, however, a very convenient way to ensure all Users that should have access to Cherwell have a User record created without the need to compile a list, assuming that AD Group membership is correct and up-to-date.

Portal Users (Customers)

Portal Users are created from the Client Application. This is a key difference, and it is important to note that manual creation of Customers in CSM can be delegated to Technicians, so as to reduce the workload on system Administrators. There is a Group Object in Cherwell called Customers, and this table contains all non-licensed Users in the system. Individual User types can be designated by creating additional Group Member Objects (through the Administration application), so that the organization can delineate between employees, contractors, vendors, etc. This can be very useful for highly complex organizations that need to provide access to a wide variety of end users and control their user experience and access to various parts of the system.

Customer records, like User records can be created by import from an external data source or by manual entry. However, unlike Licensed Users, Portal Users can be imported *en masse* from an LDAP source. This makes it very trivial to set up a scheduled import/update of all Customer records in the system, thus further automating access and security.

There is also an additional step to provide access to the self-service portal to each of these User records. This step involves setting the Security Group and credentials the User will use to access the self-service portal. This can be done manually for individuals or for a group as a batch process. Also, because the batch process can be scheduled against a specific search group, different User types can be placed in different Security Groups.

And this is where having multiple Customer Group Member Objects can be critical. As can be seen in Figure 6, breaking the Customer Group into smaller Group Member Objects can provide a simple way to logically separate different end user groups into Security Groups. And each of these Security Groups can be given access to different types of records within Cherwell. For example, Vendors may be restricted to only viewing Purchase Orders and Invoices, while Employees and Contractors will
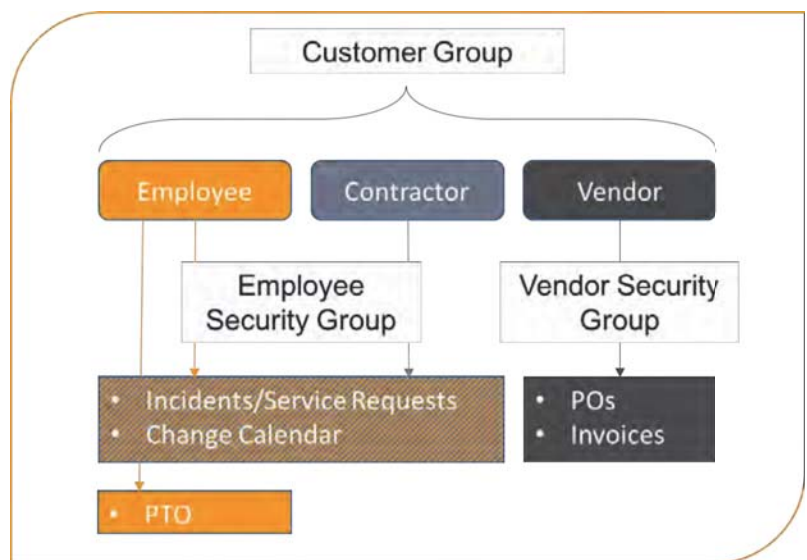

Figure 6

have access to create/modify Incidents and Service Requests. Additionally, based on the actual Group Member Object in use, additional records can be provided, such as giving Employees access to personal time-off records.

3.4.4 Summary
- There are two types of Users in Cherwell, Licensed Users (Technicians) and Portal Users (Customers);
- Users can be imported from an external data source, such as an LDAP system, or they can be manually entered;
- Licensed Users can only be imported one at a time; Portal Users can be imported as a batch job;
- If an external authentication system, such as Microsoft® Active Directory, is used, only the username needs to be stored in Cherwell;
- Portal Users must be given access to the self-service portal through an additional step, which can be scheduled and run as a periodic batch job;
- Multiple Customer types can be created within Cherwell to provide various levels of access and user experience to different types of Users.

4 Security Properties

Beyond the various tiers of security within Cherwell, there are also specific right within the tool itself that can be granted or revoked. These are simply referred to as 'Rights' and they are varied and highly granular. Each specific right has one of two constructs. Either the Right is Boolean (grant/deny), or it is more nuanced. The secondary construct consists of the following: Allow, View, Add, Edit, and Delete. These constructs are dependent on the type of Right in question, and can be expanded based on context. The second portion of this section is dedicated to Business Object Rights, which have been discussed at some length in previous sections, but they will be further broken down here for clarity.

4.1 Rights

4.1.1 Purpose
Rights govern the various activities any given User can perform within CSM, based on Security Group Membership. This includes everything from the ability to access the application to whether or not a User can directly modify data definitions using the Definition Editor.

4.1.2 Best Practice
The number of Rights that can be controlled within Cherwell is too vast to fully cover in this paper; however, there are some basic Rights which should be mentioned, as they are key to some basic security principles within the system.

Run the Application

This Right is as basic as it gets, and it is important to ensure that all Licensed Users can access the Cherwell Client application in order to dispose of records properly. It is not necessary to ensure that this Right is denied to Portal Users, since logging into the application requires a Licensed User account, but it is good practice to deny the Right to those Security Groups that do not need access to the Cherwell Client.

Table Management

This is a very tricky Right, but it is generally considered good practice to limit access to lookup tables in the Cherwell Client application to Administrators, or possibly to a 'junior' Administrator Security Group in order to minimize the impact that can be realized by making changes to data validation tables.

System Blueprints

Blueprint creation, modification and publishing should be limited to Administrators, or possibly to a Junior Administrator, as needed. Regular Technicians have no need to create or access Blueprints, and modifications should be placed under the organizations Change Management process.

Dashboards (and Widgets)

This is a set of Rights that should be discussed at length and decisions made based on the organization's level of confidence in its User community. The ability to create and maintain Team, or even personal, dashboards and widgets can be very useful for Technicians; however, it is also important that the organization ensure that key performance indicators are being presented to the appropriate Users. Providing access to this set of Rights should be approached with thoughtful consideration.

There are many other Rights which each individual Organization will need to review and assess on a case by case basis, and this list is only meant to be a launch point for Administrators.

4.1.3 Configuration

System Rights are configured per Security Group, much as Business Object Rights (detailed below). They must be modified and managed from the Cherwell Administrator application, in the Security section. Once Rights are modified, it requires affected Users to log out and back into the system, so it is generally good practice to perform these modifications during low usage times to ensure greater coverage of the User base. It is also possible to lock the system when making these sorts of changes; however, this is not always a viable option if the organization runs a 24/7 Service Desk.

Each Right group generally has multiple Rights that can be configured, and each Right is noted by an icon indicating which construct it is using (green check/red 'x' for allow/deny and a small padlock for complex settings). The constructs are laid out as checkboxes, so it is very easy to see each setting as the Right is selected. There is no way to export this list of settings, so an Administrator must go through each Right group individually to record and maintain each Right.
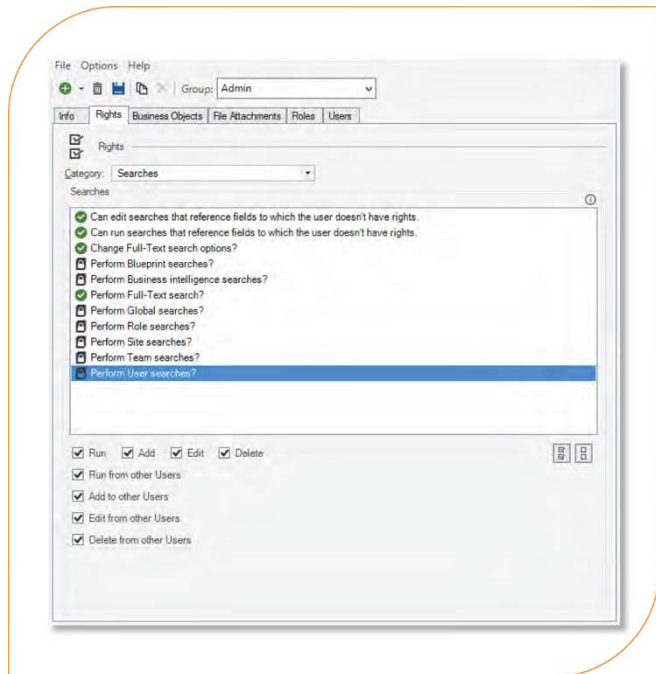

Figure 7

4.1.4 Summary
- Rights control what activities members of each Security Group can and cannot perform within the system;
- Rights are combined into Rights groups for ease of administration;
- Some Rights are Boolean in nature, while others offer more complex configuration settings;
- Rights must be set individually for each Security Group in the system

4.2 Business Objects

4.2.1 Purpose
Security settings for Business Objects makes it possible for Administrators to very tightly control what tables can be accessed and modified, as well as providing field level granularity as it relates to visibility, editing, and even deleting records within CSM. Because data is at the heart of everything we do in Cherwell, this is likely the most widely configured area of security within the system.

As a system is configured and matures, Administrators will find themselves returning to this portion of the tool frequently to update how Users interact with the system based on Security Group, Role and even Team membership.

4.2.2 Best Practice
The Business Object security section is comprised of two basic levels, Object Security and Field Security. Each Security Group can be configured to have very general rights associated with each Object, or an Administrator may need to get extremely specific with some Objects. For the most part, the out of the box configuration should work as a good starting point for each default Security Group. As has been mentioned elsewhere in this paper, it is always recommended that an existing Security Group is duplicated to create

a new one, so that an Administrator does not need to go through each and every setting individually, instead depending on existing settings to make things substantially easier. This is not to say that each setting should not be reviewed.

Each Object and the general section, has a setting for New Fields and New Objects, respectively. These can be used to set general access to both existing and new fields and objects in the system. This should be used sparingly, as often it is important that newly created fields are not open to all Security Groups equally. However, if a certain Security Group, such as Administrators, needs access to every field in every record, it is appropriate to set access rights at this level. Keep in mind that, especially as it relates to New Objects, this will allow or deny access for every new table added to the system. One of the most infuriating mistakes Administrators can make is to forget that most lower level technicians, and especially Portal Users, will not have access to newly created objects and fields, and thus will not be able to fill out new forms in the self-service portal.

If it is determined that more complex security is necessary for a specific Business Object—as is often the case with the Incident object—ensure that security is being updated for all impacted Security Groups. When using custom expressions to allow access to certain records, remember that security is written in the affirmative, meaning that every group that requires a specific type of access will need to be updated. It is not enough to simply write the expression for one Security Group. All groups must be modified.

4.2.3 Configuration

Business Object security is configured from the Administrator application. Much like system Rights, it is comprised of groupings, in this case by Business Object. Each object is broken down into its individual fields. Field structure and attributes are not, for the most part, taken into account, except as it relates to encryption. At the Business Object level, the New Field setting will appear first in the list, and as previously discussed, this controls all existing fields and any new fields created for that object. There is,
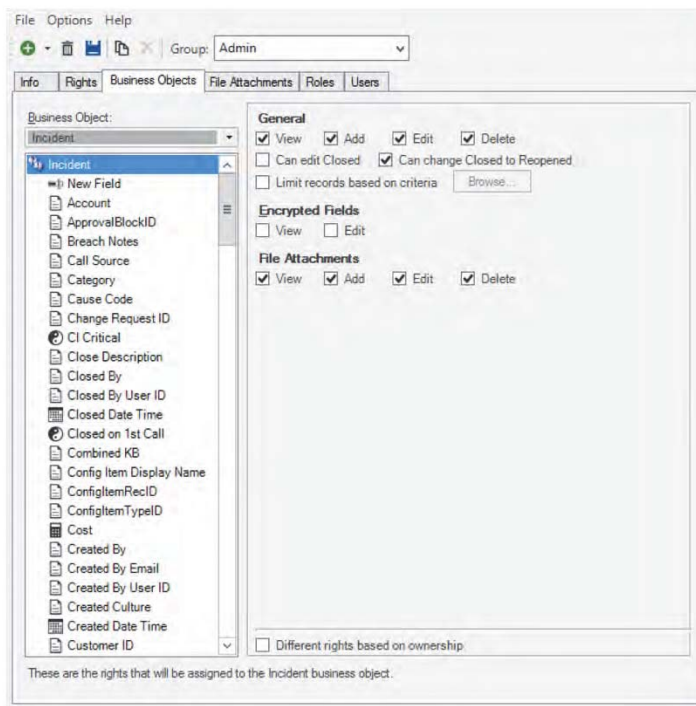

Figure 8

however, an exception to this rule. It is possible, by modifying a field's security attributes, to 'de-couple' a field from the New Field setting. Once an individual field's attributes differ from those that are set in New Field, it will no longer update alongside the New Field settings. In order to re-align a field with the New Field settings, its attributes must be matched to those of New Field, and then it will follow the New Field settings going forward. This allows Administrators the ability to provide a general security setting, but maintain the possibility of setting a few fields with custom attributes.

There are several settings for each Business Object, General, Encrypted Fields, and Attachments. If a Business Object has a defined lifecycle, there will be additional attributes for handling modifications for records that are in an archived, or read-only, state. These should generally be restricted for all Users except Administrators, in order to maintain the integrity of closed/archived records.

This is also where an Administrator can decide whether an object should be governed by ownership. A checkbox to allow different rights based on ownership is available for each Business Object. Once checked, an expanded list of attributes for each level of ownership is presented. Any attribute that is checked at the top level will be automatically selected and greyed out in each ownership section. In order to customize that attribute, it must first be unchecked at the parent level.

The ownership terms are as follows:

Record Owner: This is the User that has the attribute of 'Owner' for the record. It is usually the name stored in the OwnedBy field in out of the box configurations.

Department Member: As discussed in the User section, above, this value is set on the UserInfo record. Each User can be a member of exactly one Department, and that value is used in this attribute group to control access to a Business Object or Field.

Figure 9

Manager of Owner: This value is also maintained on each User record. Each User can have exactly one Manager, and that value is used here.

Team Member: This value represents any member of the Team that owns the record. This value is an attribute set on each Business Object, and is generally represented by the field OwnedByTeam in out of the box configurations.

Team Manager: This attribute is set for each individual User in the system. Any User can be flagged as the Manager of any Team of which he/she is a part.

Ownership based security only pertains to the ability to view, edit, create and/or delete a record, and it does not govern attachments or encrypted fields. These attributes are set for each Security Group, regardless of record ownership.

Ownership based security is also available at the field level, though there are only two attributes that can be set for each field, view and edit.

4.2.4 Summary
- Business Object Security controls access to each table and all of its fields in the system;
- General security can be set for all Business Objects and/or all fields for each Security Group;
- Each Business Object has unique settings for record access, attachments, and field encryption;
- Each Business Object can have ownership specific security settings;
- Each field within a Business Object can also have ownership specific security settings.

5 Security Accessories

Cherwell has several accessories to assist in maintaining and controlling security within the system. In addition to those discussed below, Cherwell also provides key-based security for API integration and file attachment security. These concepts are beyond the scope of this paper.

5.1 Authentication Methods

5.1.1 Purpose
Cherwell provides for basically three (3) types of authentication to the platform: 1) local user credentials, 2) LDAP authentication, 3) SAML authentication. Each has its pros and cons, and often all three are leveraged in a single system.

Local Authentication
Local users will always exist in Cherwell. Service accounts must be local should connectivity to any external authentication source fail. These accounts include the general administrator account, and each of the accounts for automated business processes and e-mail monitoring.

LDAP Authentication
This method is almost ubiquitous now, and it generally comes in the form of Active Directory integration. Cherwell has a native integration with Active Directory, which makes configuration of this authentication type very simple.

SAML Authentication

This is the newest authentication type provided by Cherwell. This allows for what is known as federated authentication, where an external, third party system, handles authentication through a secure handshake/token exchange. Since the advent of Microsoft® Azure and Active Directory Federated Services (ADFS), this method has become increasingly popular since its introduction in 2012. Most new clients are using federated authentication, and this option makes it very easy to set up externally facing systems.

5.1.2 Best Practice

What type of authentication an organization uses is nearly always governed by what is available. Most companies leverage some sort of LDAP system, and that is generally in the form of Active Directory. And, as mentioned, SAML is becoming increasingly popular as the race for the cloud intensifies. However, it is usually deciding how much of each type of authentication should be used, rather than what type. As discussed, there must be at least 2-3 local service accounts within Cherwell to handle administration and automated services. But it is likely also a good idea to configure both AD and SAML as a more redundant way to handle authentication. The biggest advantage to using AD is also the ability to schedule imports of Users on a periodic (usually daily) basis. This is especially true if the user base is in the thousands, or even tens of thousands.

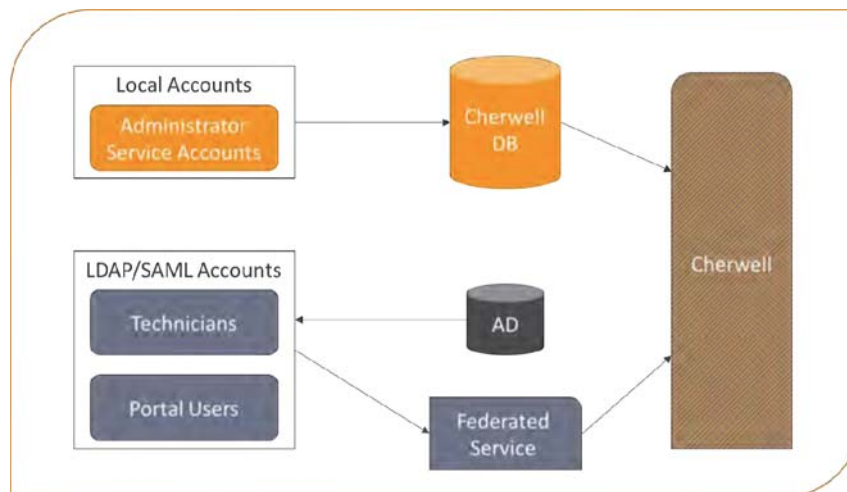A typical model might look something like this:

Figure 10

In this case, the system is using local accounts for administration and automated processes, while it is fed User data from Active Directory, and then utilizes a federated authentication service (such as ADFS) to authenticate most users into the system. This is a very efficient model, and it lends itself well to both secure, internal systems and public facing systems. It is especially effective for SaaS implementations, where the system is remote to the organization and only available over the internet.

5.1.3 Configuration

Local authentication does not require a great deal of configuration, as it is natively supported. In this model, a username and password must be manually created for each Licensed User, and portal credentials must also be manually created for each customer account.

For LDAP configuration, configuration is done from the Administrator application as part of a Blueprint. In order to set up LDAP, a service account with browse privileges to the LDAP structure must be added, and the schema path to the organizational unit (OU) where the user records are stored must be known. Cherwell supports both LDAP and LDAPS (which requires a secure certificate on the source system). Once established, both Licensed Users and Portal Users can be imported from the LDAP system. It is also advisable to set up a periodic update of Portal Users from the LDAP source system in the Cherwell Scheduler. Licensed Users must be imported *ad hoc* and cannot be automatically updated from the source system.

SAML configuration requires the use of shared certificates and metadata between the Cherwell system and the federated system. There is ample documentation available from Cherwell on setting up SAML for use with Active Directory Federated Services (ADFS), which is the most commonly used identity provider for a SAML implementation. Cherwell supports all Shibboleth v2 compliant federated systems. Each organization's SAML administrator will be able to configure and provide the necessary data and certificates to allow their system to accept SAML authentication as an identity provider. SAML is very straightforward to configure in Cherwell, requiring only the XML metadata file from the identity provider, as well as the redirect URI, to complete.

5.1.4 Summary
- There are 3 distinct types of authentication supported within Cherwell: Local, LDAP, and SAML
- Local authentication requires that username/password combinations are stored in the Cherwell database
- LDAP and SAML authentication require that only a login name be stored in the Cherwell database; actual authentication is passed off to the source system, making for a more secure, easier to maintain, authentication model
- Cherwell supports both LDAP and LDAPS
- Cherwell supports all Shibboleth v2 compliant SAML identity providers

5.2 Field Level Encryption

5.2.1 Purpose

The final security concept presented in this paper is field level encryption. Cherwell has always encrypted data transfer in motion, but until recently, data encryption at rest was only available at the database level, using SQL tools. However, with more recent versions of the tool, field level data encryption has become part of the platform. This is a key

concept for many regulatory requirements, such as HIPAA, FERPA and PCI compliance. At rest data encryption shows Cherwell's commitment to increasing security demands in each organization, and as with all of CSM's security concepts, it is a very configurable element of the platform.

5.2.2 Best Practice

At rest data encryption at the field level should be used only where necessary. Such encryption limits the ability of the tool to report on field values, and if it is overused, it can make the tool much less usable. However, where such encryption is necessary, whether to meet organizational standards or regulatory requirements, it is an extremely useful tool in the Cherwell Administrator's toolbox.

The most common use of field level encryption generally revolves around personally identifiable information (PII). This can be something as seemingly mundane as a user's home address and/or phone number, up to and including a Social Security Number. But it can be used for other sensitive data as well. Consider the earlier examples of using the Cherwell platform for HR processes. Field level encryption could be used to mask salary information, employee review data, or even termination notes. None of these are governed by external regulations, but most organizations (and their employees) would certainly prefer to keep this data private.

Encrypted fields should not be used for data that ought to be shared between many different individuals. There is never a need to mask the information in a Service Request if it needs to be accessed and acted upon by possibly multiple resources within the organization. This simply adds overhead that is not necessary, and it makes such data impossible to report upon. It is advisable to discuss and come to consensus on which fields should and should not be encrypted, and then train users to utilize encrypted fields for sensitive data, and to leave things like PII out of open fields like request descriptions and work notes.

5.2.3 Configuration

Encrypting any field is as easy as checking a box in that field's properties within a blueprint. All data in that field will instantly be encrypted. Allowing access to encrypted fields is nearly as simple, and it is configured from the Security Group Business Object properties in the Security section of the Administrator tool. Each Security Group can be allowed or denied visibility and edit rights of encrypted data fields. This configuration is at the Business Object level, so if view and/or edit rights are granted to a Security Group for an object, such as Incident, then members of that Security Group would be able to view and/or edit any encrypted field in that table.

Once a field has been encrypted it is no longer available to reports and dashboards, so it is important to keep this in mind during design. Additionally, if a User is granted view or edit rights, the encrypted fields must be placed on the object's form in order for anyone to decrypt or modify the data contained within an encrypted field.

5.2.4 Summary

- Cherwell encrypts all data 'in motion' within the application;
- Field level encryption (or data encryption 'at rest') is a recent addition to the CSM platform;
- Field level encryption can be used to secure PII and other regulatory data, as well as organizational data that is deemed sensitive;
- It is good practice to limit encryption to those fields that truly require it;
- Any individual field can be encrypted;
- Security to allow view/edit for encrypted fields exists at the Business Object level;
- Encrypted fields are not available for reporting or dashboards.

6   Conclusion

Cherwell's four-tiered security model provides vast possibilities for allowing and constraining access to nearly every aspect of the toolset. Because each level can be configured independently, Administrators are able to pinpoint access to everything from the application itself to individual fields within a single table in the database, and almost anything one could dream up in between. By leveraging Security Group membership, the tool can provide specific user experiences based on function within the organization, making Cherwell much more than just an ITSM tool. Roles give an administrator the ability to present wholly different forms and dashboards to each type of user in the system. And Team membership makes it possible to quickly delegate responsibility to groups of users automatically.

The flexibility of the basic security model coupled with the granularity provided by system and object rights is truly second to none in the industry today. Each action that can be performed is configurable at the individual user level, if necessary, and access to entire sections of the platform can be tightly controlled and maintained.

Add to this the multiple ways the system can be accessed, leveraging existing authentication technologies and natively integrating with industry standard protocols, and Cherwell demonstrates its full potential from a security standpoint.

Configuring each aspect of security within Cherwell is a complex task, and it should be undertaken with a great deal of planning. Each organization is different and has varying security requirements. However, with the vast array of tools available within the CSM platform, it is possible to meet these requirements and provide a useful, highly secure toolset that can be used across the enterprise.

Appendix C) Cherwell Software US Hosted Environment

See following pages for Cherwell's US Hosted Environment Document.

Appendix D) Cherwell Security Whitepaper for North America

See following pages for Cherwell's Security Whitepaper for North America.

Appendix E) Case Studies

See following pages for case studies highlighting our customers experiences working with Beyond20 and Cherwell Service Management.

CUSTOMER SUCCESS
STORY

OneNeck®
IT SOLUTIONS
a TDS® Company

**"WE COMPLETELY
TRUST THE PEOPLE
WHO ARE WORKING IN
OUR ENVIRONMENT."**

-- STEVE BAZINET

As a provider of hybrid IT solutions tailored for mid-market and enterprise companies, OneNeck® IT Solutions knows something about the importance of delivering IT services through an integrated platform, and ensuring all users are working with the most up-to-date version of those services. That is the type of corporate intelligence that has helped the Scottsdale, AZ-based subsidiary of Telephone and Data Systems grow into a 650-employee organization with clients around the world.

Yet OneNeck, like many other companies focused on business-critical missions, has not always found it easy to achieve integration and upgrades in its own IT Service Management (ITSM) software. The organization had invested in three ITSM systems, including a proprietaty solution the company developed in-house. Over time, these tools became out of date and limiting; OneNeck found itself several iterations behind the most recent upgrades to the point a fresh integration was the only way to go.

"That was the underlying factor for us to look at changing platforms," said Steve Bazinet, Director of Business Applications for OneNeck. "We were looking for a new platform that could consolidate all of the service desk tools throughout our different locations. We began investigating options and that is when we learned about Cherwell."

THE SOLUTION

What most impressed Bazinet about Cherwell was the long-term savings OneNeck could achieve in managing and maintaining the ITSM software. "Because of Cherwell's codeless environment, we could make enhancements to the system without having to hire java developers. That was probably the biggest factor, but we also appreciated the ease of upgrades, particularly that we could do upgrades without losing customizations."

OneNeck initially went live with Incident Management, quickly adding Change, Problem, and Configuration Management. Within two months, OneNeck had migrated 99.9% of its customers to Cherwell. The development process posed some learning curves for the organization, but Bazinet says BEYOND20's support and assistance proved invaluable.

"They've been very responsive to our needs at every step," Bazinet said. "We completely trust the people who are working in our environment."

THE RESULT

The Cherwell solution has proven to be a wise investment for OneNeck. Bazinet appreciates the ease of adding and modifying custom modules to the platform using the Mergeable Application (mApp) Exchange, thus eliminating the time and expense of building each new system change from scratch. He also has found Cherwell beneficial in that it has allowed for automation and integration of email management.

"Previously, I had to copy and paste email from my own client into our IT service management systems because they were so outdated we couldn't receive emails directly in them," Bazinet said. "We estimate that eliminating manual handling of email from our service desk alone will save us approximately $300,000 a year - and that only accounts for one-fifth of the users of the system

THE FUTURE

Bazinet says the plan now is to develop a metrics dashboard so managers can monitor how their teams are performing in areas such as incident response and resolution time. The sales team is also exploring the potential to automate the sale of low-dollar items through the portal, thus benefiting customers by eliminating the need for paperwork. OneNeck is exploring additional opportunities to realize its corporate vision through the Cherwell platform and excited about how this platform can support the organization in its continued growth.

CUSTOMER SUCCESS STORY

METRO CREDIT UNION

QUICK WINS

- REAL-TIME DASHBOARDS
- CONSISTENT, EASY-TO-MANAGE BUSINESS PROCESS WORKFLOWS
- IMPROVED COLLABORATION & INTEGRATION ACROSS BUSINESS UNITS

"IT'S VERY EASY TO MANAGE THE SYSTEM, AND BEYOND20 HAS PLAYED A LARGE PART IN MAKING THAT POSSIBLE."

For nearly 100 years, Metro Credit Union has helped its members achieve their financial goals through exceptional service and guidance. It is a commitment that has made the nonprofit financial co-op the largest state chartered credit union in Massachusetts, with $1.7B in assets and 190,000 members.

Yet, there was a time when Metro Credit Union found itself in need of some guidance to maintain that impressive legacy. For years, the organization had tracked every aspect of the audit + exam process - from scheduling to final reports - using Excel. It had become clear that this approach was no longer sufficient to meet their needs in keeping up with regulatory requirements.

"There was no real workflow," explains Traci Michel, Senior Vice President of Operations within Metro Credit Union. "Everything was manual and tracked in spreadsheets, and those were passed around via email. That made accountability difficult because we could not be sure that people were consistently updating those spreadsheets to indicate where they were in a particular audit process. We wanted to track deadlines and progress, so we started looking for a way to do this more efficiently."

PMI Project Management Institute — Registered Education Provider

Cherwell SOFTWARE PARTNER™

Microsoft GOLD CERTIFIED Partner

ITIL TRAINING ORGANIZATION ACCREDITED BY ACQUIROS ON BEHALF OF AXELOS

GSA Contract Holder

BOMGAR | Gold Partner

THE SOLUTION

The consensus at Metro Credit Union was that Cherwell's platform was best suited to meet the organization's requirements, not just because it would make tracking of auditing and exams easier but also because it could be wrapped into other business units, such as Human Resources and IT. But Michel says it was Beyond20's expertise and support that illustrated how the software could meet, and ultimately exceed, Metro Credit Union's expectations.

"We realized pretty quickly just how adept the Beyond20 team is when it comes to helping you use this platform," Michel says. "Through Q&A sessions and whiteboarding, they were able to capture our key requirements for the audit tracking process and then they used that information to help us learn all about the technology so we could become fully self-sufficient in managing and supporting the platform."

Michel notes that Beyond20 played a key role in helping Metro Credit Union employees adjust to Cherwell's dashboard-focused environment. "In the beginning, users were asking if they could get an email every time a particular incident happened. With Beyond20's guidance, we were able to build custom, real-time dashboards that proved to be absolutely vital in viewing the current state of the organization. They helped make that culture shift possible."

THE RESULT

Once that shift occurred, the benefits of the Cherwell platform, and Beyond20's implementation support, quickly became clear. "We gained better tracking on repeat findings, which are a high priority to remediate," Michel says. "Whereas in the past it would have been a largely manual process to compile reporting, we now have that information at our fingertips, so it is very easy to pull together year-over-year comparisons."

Michel says Metro Credit Union realized that the same Cherwell software that had enhanced tracking of the audit lifecycle could lead to greater efficiencies in other business units. With help from Beyond20, the organization extended the platform, allowing HR to track each employee's lifecycle, and then track the employee's access to applications.

"We now have an end-to-end solution that tracks the request for access to an application, associates it with an individual, and then terminates that access when the individual leaves the organization. That really ties everything together, and it has prompted our team to look for the next logical process they can pull into the system."

More recently, Metro Credit Union extended the system to include a number of additional real-time dashboards, resulting in invaluable metrics that had previously been unavailable. "We realized that 20% of all of our helpdesk tickets were created for password resets, and that enabled us to look at how we could offer enhanced self-service password reset options. It will free our IT team to focus on more vital initiatives, so having those metrics enables us to make better business decisions about how we allocate resources."

THE FUTURE

The Cherwell platform continues to benefit Metro Credit Union in many ways, from improved collaboration and integration across business units, to better metrics on system downtimes that help prevent reoccurrences. The organization is looking to extend the software into other areas, such as providing a one-stop shop for all internal operational ticketing. Michel says the Cherwell solution, coupled with Beyond20's support, will be crucial to Metro Credit Union's growth.

"What's been fantastic about the software is that it scales. I do not need to make major changes to it so that it continues to work for us as we grow. All it takes is a tweak. It's very easy to manage the system, and Beyond20 has played a large part in making that possible."

Appendix F) Resumes

See following pages for resumes of the following key personnel.

- Lauren Foiles – Project Manager
- Larry Martin – Solutions Architect
- Christian Greenleaf – Solutions Consultant

CHERWELL END-USER SUBSCRIPTION AGREEMENT

THIS END-USER SUBSCRIPTION AGREEMENT ("EUSA"), TOGETHER WITH ANY APPLICABLE CHERWELL ORDER CONFIRMATION FORM THAT REFERENCES THIS EUSA (COLLECTIVELY, THE "AGREEMENT"), IS BETWEEN CHERWELL SOFTWARE, LLC, A DELAWARE LIMITED LIABILITY COMPANY ("CHERWELL"), AND THE CUSTOMER IDENTIFIED ON THE ORDER CONFIRMATION FORM ("CUSTOMER"). THIS AGREEMENT CONSTITUTES THE ENTIRE AGREEMENT BETWEEN CUSTOMER AND CHERWELL REGARDING THE CHERWELL SOFTWARE PRODUCTS ("LICENSED SOFTWARE") AND THE MAINTENANCE AND SUPPORT AND PROFESSIONAL SERVICES THAT ARE LISTED ON THE ORDER CONFIRMATION FORM. BY INSTALLING OR USING THE LICENSED SOFTWARE, CUSTOMER ACKNOWLEDGES THAT IT HAS READ AND AGREES TO ALL OF THE TERMS AND CONDITIONS CONTAINED IN THIS AGREEMENT.

1.   GRANT OF LICENSE AND SUBSCRIPTION

1.1   Subscription License. The Licensed Software, which includes all configurable and executable application content or "Blueprints," is licensed to Customer for use subject to the terms of this Agreement. Cherwell hereby grants to Customer and Customer fully accepts, upon delivery, a nonexclusive, non-transferable right to access and use only the executable version (no source code) of the Licensed Software, during the term of the Subscription Service, as described below (the "Subscription Service"). This is not a perpetual use license; rather, Customer is using the Licensed Software pursuant to the Subscription Service and for a limited duration. Customer is allowed only the number of concurrent users of the Licensed Software as shown on the Cherwell Order Confirmation Form. If Customer wishes to expand the number of authorized concurrent users covered by the license, Customer can purchase additional user licenses. Customer's authorized concurrent users of the Licensed Software can include Customer, its subsidiaries and affiliates, and their employees and authorized representatives, agents and contractors. Customer may install copies of the Licensed Software in non-production environments, for purposes of testing, development or disaster recovery, provided, however, that such copies cannot be used for production purposes and there cannot be more than one installation of the Licensed Software in a production environment. In no event shall the number of concurrent users in a production environment exceed the authorized concurrent users covered by the license.

1.2   CHERWELL ASSET MANAGEMENT

**1.2.1   **If purchased by Customer, the term Licensed Software shall include the Cherwell software product known as Cherwell Asset Management ("CAM Software"), which includes, but is not limited to: (a) the Cherwell proprietary application database ("Cherwell Software Identification Database™" or "CSID™") and the data accessed by and/or contained therein, (b) the Logi Analytics, Inc. proprietary software product known as "Logi Info Server", (c) the reports generated by use of CAM Software, and (d) CAM Software product documentation. Notwithstanding anything to the contrary in this Agreement, Customer shall have the right to terminate its subscription license of the CAM Software after one year from the Effective Date (as defined below). For the avoidance of doubt, termination of the subscription license of the CAM Software shall not terminate Customer's subscription license of the other Licensed Software.

**1.2.2   **With regard to CAM Software, Customer acknowledges and agrees that it may install a copy of the CAM Software on a network server(s), provided that Customer acquires and dedicates a license for each computer workstation on the network(s) on which the CAM Software will be used. The CAM Software is "used" when it is loaded in temporary or permanent memory of a computer. In addition, Cherwell grants to Customer a limited, personal, non-transferable and non-exclusive right to use the CAM Software in connection with a server, application server, or desktop application virtualization technology. This includes but is not limited to Citrix®, Microsoft Terminal Server®, or VMWare® technologies that are capable of creating multiple virtual machines or sessions on which the CAM Software can be run. Customer must acquire and dedicate a license for each such machine, virtual machine, or session running a separate instance of the CAM Software.

1.2.3   The CSID may be installed on servers solely for use in conjunction with Customer's licensed copies of the CAM Software, in accordance with the product documentation.

1.3   **Subscription Service Term.** This Agreement is effective as of the earlier of the date Customer first uses or installs the Licensed Software or the date set forth on the Cherwell Order Confirmation Form (the "Effective Date").   Customer's right to use the Licensed Software continues until this Agreement is terminated or the Subscription Service expires.   The Subscription Service is offered on no less than an annual basis and will commence and be invoiced in advance of each annual period to Beyond20... Subscription fees increase as Customer adds additional concurrent user licenses.   Either party may terminate this Agreement upon written notice to the other party if the other party fails to cure a material breach of this Agreement within thirty (30) days of written notice of the breach from the terminating party.   Upon any termination, Customer agrees to remove all Licensed Software from its computers, destroy all copies of the Licensed Software, and, upon request from Cherwell, certify in writing its compliance.   Upon termination by Customer for an uncured breach by Cherwell, Cherwell will pay Customer a pro rata refund of any prepaid but unused Subscription Fees.

1.4   **Intellectual Property Rights.** The Licensed Software is protected by copyright and other intellectual property laws.   Cherwell retains all rights, title and interest in and to the Licensed Software. Customer agrees that this is a license only and that no title passes to Customer.   If Customer makes or installs copies of the Licensed Software as provided in this Agreement, the original and all copies of the Licensed Software may not leave Customer's control and are owned by Cherwell.   Customer retains all rights to its data.

1.5   **Restrictions.** To the maximum extent permitted by applicable law, Customer may not resell or otherwise transfer for value the Licensed Software without the written consent of Cherwell.   Customer may not export, ship, transmit, or re-export the Licensed Software in violation of any applicable law or regulation, including, without limitation, the Export Administration Regulations issued by the United States Department of Commerce and the United States trade embargoes and economic sanctions administered by the U.S. Treasury Department, Office of Foreign Assets Control, or any such similar law or regulation issued by such other governmental entity which may have jurisdiction over such export.   Customer agrees not to: (i) modify, decompile, disassemble or reverse engineer the object code portions of the Licensed Software; (ii) distribute, rent, lease or lend the Licensed Software; or (iii) use the Licensed Software except as expressly permitted under this Agreement.

2.   **INDEMNIFICATION**
2.1   Cherwell shall defend, indemnify and hold Customer harmless against all third party claims, suits, proceedings, costs, damages, losses and expenses (including reasonable attorneys' fees), and judgments incurred, claimed or sustained by Customer arising out of or related to any allegation that any portion of the Licensed Software (including any updates, error corrections, or upgrades thereto), when used solely in the manner and for the purpose for which it was licensed hereunder, violates any patent, copyright, trade secret, trademark, or other third party intellectual property right.   If a claim is filed in a court or other administrative proceeding seeking to enjoin the use of the Licensed Software, Cherwell shall either: (i) at Cherwell's cost, procure for Customer the right to continue to use the relevant portion of the Licensed Software; (ii) replace, at Cherwell's cost, the relevant portion of the Licensed Software with a substitute product that functions substantially in accordance with the applicable specifications for that portion of the Licensed Software; or (iii) at Cherwell's cost, modify the Licensed Software so that it does not infringe or misappropriate, provided that the Licensed Software, as modified, continues to perform substantially in accordance with the applicable specifications.

2.2 Cherwell's indemnification obligation pursuant to the above shall not apply to the extent any infringement claim is found to be caused by (i) Customer's use of the Licensed Software in a manner that is not provided for under this Agreement or Cherwell's user documentation; or (ii) Customer's use, operation or combination of all or any component or portion of the Licensed Software with all or any portion of other software, equipment or systems not provided or required by Cherwell. As a condition precedent to any liability of Cherwell, if Customer receives notice of any infringement claims for which indemnification may be available under the above, Customer must promptly notify Cherwell in writing of the infringement claim.

2.3 Cherwell will have the right to control the defense, select counsel, and direct the course of resolution, including settlement of any infringement claim (but only if the settlement does not include an admission of liability by Customer, does not involve more than the payment of money and grants Customer a full and unconditional release from all liability with respect to the claim). In addition to the defense provided by Cherwell, Customer may elect to retain its own counsel, but Cherwell will not be responsible for any fees or expenses of such counsel.

3. WARRANTIES AND DISCLAIMERS

3.1 Limited Warranties. Each party represents and warrants to the other that it has the legal power to enter into this Agreement. Cherwell further represents and warrants that: (i) it has the right to grant to Customer the license to use the Licensed Software as set forth in this Agreement without violating any rights of any third party and that, to the best of Cherwell's knowledge, the Licensed Software does not infringe or otherwise violate any intellectual property rights of any third party; (ii) the Licensed Software shall operate in material compliance with Cherwell's user documentation; (iii) all services provided by Cherwell pursuant to this Agreement relating to the Licensed Software will be performed in a timely and professional manner, by qualified and skilled individuals, and in conformity with standards generally accepted in Cherwell's industry; and (iv) the Licensed Software shall be delivered free of any virus or otherwise malicious code, or any code or command intended to bring down the Licensed Software or Customer's computers/networks automatically or upon command or otherwise impair their use.

3.2 Limited Remedy. In the event of any breach of warranty, Customer's sole and exclusive remedy shall be for Cherwell to either correct or replace, at no additional charge to Customer, any portion of the Licensed Software or services found to be defective or, if Cherwell is unable to correct or replace the defect, refund any prepaid but unused Subscription Service fees paid by Customer; and in the event Cherwell introduces any virus or such disabling code or commands into the Licensed Software or any of Customer's equipment, make commercially reasonable efforts to restore any and all data or programming lost by Customer as a result of such virus or disabling code.

3.3 Disclaimer. TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, THE WARRANTIES SET FORTH IN SECTION 3 ARE EXCLUSIVE AND IN LIEU OF ALL OTHER WARRANTIES, ORAL OR WRITTEN, EXPRESSED OR IMPLIED. CHERWELL DOES NOT WARRANT THAT THE OPERATION OF THE LICENSED SOFTWARE WILL BE UNINTERRUPTED OR ERROR FREE. EXCEPT AS SET FORTH IN THIS SECTION 3, CHERWELL MAKES NO WARRANTY OR REPRESENTATION, EITHER EXPRESSED OR IMPLIED, WITH RESPECT TO THE LICENSED SOFTWARE, ITS QUALITY, PERFORMANCE, MERCHANTABILITY, OR FITNESS FOR A PARTICULAR PURPOSE.

4. LIMITATION OF LIABILITY; EXCLUSION OF DAMAGES

4.1 Limitation of Liability. To the maximum extent permitted by applicable law and except for Customer's payment obligations under this Agreement and Cherwell's obligation to indemnify Customer under Section 2, each party's entire liability under this Agreement shall be limited to three times the amount paid by Customer for the Subscription Service during the most recent twenty-four (24) month period, which shall not include any amount paid for related or Professional Services.

This limitation of liability shall not affect Cherwell's indemnification obligations hereunder, warranty claims, or claims not covered under an insurance policy.

4.2   Exclusion of Consequential and Related Damages.   TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, IN NO EVENT SHALL EITHER PARTY BE LIABLE TO THE OTHER FOR LOST PROFITS, LOSS OF USE OR INDIRECT, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES, WHETHER IN CONTRACT, TORT OR ANY OTHER THEORY OF LIABILITY, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGES, EXCEPT TO THE EXTENT THAT ANY THIRD PARTY CLAIM SUBJECT TO INDEMNIFICATION UNDER SECTION 2 INCLUDES SUCH DAMAGES.

5.   MAINTENANCE AND SUPPORT AND SERVICES

5.1   General. The Subscription Service includes Maintenance and Support of the Licensed Software. Failure to pay any amount due under this Agreement may result in suspension of Maintenance and Support.   If Maintenance and Support is interrupted as a result of expiration or termination, Customer may be charged a reinstatement fee equal to the cost of Maintenance and Support for the period from the date of expiration or termination to the date of renewal.

5.2   Maintenance. "Maintenance" entitles Customer to receive updates, upgrades, patches, bug fixes and new releases or versions of the Licensed Software, including updated documentation, as Cherwell may provide from time to time without requirement of a separate license agreement, and without additional charge other than payment of the Subscription fee.

5.3   Support. Where provided by and purchased from Cherwell, "Support" entitles Customer to technical assistance with Customer's ongoing use of the Licensed Software, 24 hours a day, 7 days a week. Cherwell will provide support for the most current version of the Licensed Software and one prior version, including interim releases between the two versions; for example, upon release of version 5.x Cherwell will support version 5.x and 4.x. Cherwell may provide limited support for older versions. Cherwell will use its best efforts to answer Customer's specific questions and provide support in accordance with Cherwell's service and support guidelines. Support does not include any third party products that are not part of the Licensed Software.   If Support is purchased from and provided directly by a Partner, as described in Section 7.7 below, then the terms and conditions of any agreement between Customer and Partner shall govern with regard to Support.

5.4   Professional Services. Where provided by and purchased from Cherwell, "Professional Services" may include training, implementation, installation, on-site assistance, customization, and configuration of the Licensed Software. The total "Professional Services" fee quoted on the Cherwell Order Confirmation Form, if any, is an estimate of the number of days required based on Cherwell's current understanding of Customer's stated implementation requirements.   A statement of work shall be mutually agreed upon prior to commencement of any Professional Services. Any professional or related services purchased from and provided directly by a Partner, as described in Section 7.7 below, shall be governed by the terms and conditions of any agreement between Customer and Partner.

6.   CONFIDENTIALITY

6.1   Definition. As used in this Agreement, "Confidential Information" means any information, whether oral or written, designated by a party as confidential or that reasonably should be understood to be confidential or proprietary in nature. Customer's Confidential Information shall include Customer data stored or processed with the Licensed Software.   Cherwell's Confidential Information shall include the Licensed Software. Confidential Information of each party shall include the terms of this Agreement (but not the fact of its existence), as well as each party's business and marketing plans, financial data, employee data, product plans and designs, and technical information. However, Confidential Information shall not include any information that (i) is or becomes generally known to the public other than by breach of this Agreement; (ii) was known to the receiving party prior to its disclosure; (iii) becomes known to the receiving party after proper disclosure from a third party not under an obligation of confidentiality; or (iv) was disclosed to the minimum extent necessary to comply with a lawful court order or government law or regulation, including the Texas Public Information Act (currently codified under Tex. Govt. Code Chapter 552),provided that in the case of (iv) the

disclosing party shall provide the other party with advance written notice thereof and reasonably cooperate with the other party to limit disclosure and obtain protective orders or other relief as appropriate.

6.2 **Protection.** Each party agrees to hold the other party's Confidential Information in strict confidence and to treat such other party's Confidential Information with at least the same degree of care employed with respect to its own Confidential Information (but in no event less than reasonable care). Neither party shall (i) use the other party's Confidential Information for its own account or in any manner not contemplated by this Agreement; nor (ii) disclose the other party's Confidential Information to a third party without the prior written consent of the other party. Both parties shall limit access of each other's Confidential Information to those of its employees, contractors and agents who have a need for such access and who are bound to confidentiality obligations substantially similar to those set forth in this Section. This Section shall survive termination or expiration of the Agreement (for any reason) for a period of three (3) years.

7. **MISCELLANEOUS**

7.1 **Severability.** If any of the terms, or portions thereof, of this Agreement are invalid or unenforceable under any applicable statute or rule of law, the court shall reform the Agreement to include an enforceable term as close to the intent of the original term as possible; all other terms shall remain unchanged.

7.2 **Entire Agreement.** This Agreement constitutes the entire agreement between Customer and Cherwell relating to the subject matter hereof and supersedes all prior and contemporaneous agreements, representations, proposals and negotiations, whether written or oral. Any additions to, or modifications of, this Agreement shall be binding upon the parties only if in writing and executed by a duly authorized representative of Customer and Cherwell. TERMS AND CONDITIONS OF ANY CORRESPONDING PURCHASE ORDER OR OTHER DOCUMENT RELATING TO THE LICENSED SOFTWARE THAT ADD TO OR CONFLICT WITH THE TERMS CONTAINED IN THIS AGREEMENT SHALL BE DEEMED MATERIAL AND ARE REJECTED.

7.3 **Waiver.** The waiver or failure of either party to exercise in any respect any right provided for in this Agreement shall not be deemed a waiver of any further or future right under this Agreement.

7.4 **RESERVED.**

7.5 **RESERVED**.

7.6 **Choice of Law.** This Agreement is governed under the laws of the state of Texas, without regard to its conflicts of laws principles. This Agreement will not be governed by the United Nations Convention on Contracts for the International Sale of Goods, the application of which is expressly excluded.

7.7 **Third Parties and Third Party Resellers.** No person who is not a party to this Agreement has or shall have any right to enforce any term of this Agreement and no consent of any third party shall be required for any cancellation or variation of the Agreement. From time to time, Cherwell may authorize certain third parties, such as value-added resellers or solutions partners ("Partners"), to resell the Licensed Software and

Maintenance and Support Services. Customer acknowledges that as between Customer and Cherwell, Partners are not authorized to modify the terms and conditions of this Agreement nor the rights granted to Customer with regard to the Licensed Software. In certain jurisdictions or markets, Customer may purchase, from the Partner (rather than Cherwell), Support Services and Professional Services to be performed by the Partner. In such case, the terms of any agreement between Customer and Partner for such services shall govern, and Cherwell shall not be liable or otherwise responsible for Partner's performance or non-performance under such agreement. Maintenance, as described in this Agreement, shall in all cases be provided by Cherwell, subject to the terms of this Agreement.

7.8   RESERVED

Signature lines for the EUSA are located on the Cherwell Order Confirmation form to which the EUSA is incorporated by reference.

City of Austin
SMBR
Small & Minority Business Resources
Opening the door to opportunities

Buyer Name/Phone	Sai Xoomsai Purcell/512-974-3058	PM Name/Phone	Diana Heath/(512) 530-634
Sponsor/User Dept.	ABIA	Sponsor Name/Phone	
Solicitation No	RFP 8100 PAX3147	Project Name	Information Technology Service Management Software Solutions
Contract Amount	$600,000/60 month	Ad Date (if applicable)	N/A

Procurement Type

☐ AD – CSP	☐ AD – CM@R	☐ AD – Design Build
☐ AD – Design Build Op Maint	☐ AD – JOC	☐ IFB – Construction
☐ IFB – IDIQ	☐ PS – Project Specific	☐ PS – Rotation List
☒ Nonprofessional Services	☐ Commodities/Goods	☐ Cooperative Agreement
☐ Critical Business Need	☐ Interlocal Agreement	☐ Ratification
☐ Sole Source*		

Provide Project Description**

Aviation Department is seeking an Information Technology Service Management Toolset (ITSM) software solution and implementation services. The ITSM solution requires modules that cover all aspects of the Information Technology Infrastructure Library v3-2011 (ITIL) processes for IT Service Management. The solution must provide fully integrated functionality across the following stages: Service Strategy, Service Design, Service Transition, Service Operation, and Continual Service Improvement.

Project History: Was a solicitation previously issued; if so were goals established? Were subcontractors/subconsultants utilized? Include prior Solicitation No.

N/A.

List the scopes of work (commodity codes) for this project. (Attach commodity breakdown by percentage; eCAPRIS printout acceptable)

20811 - 70%, 92045 30%

Sai Xoomsai Purcell	10/25/2018
Buyer Confirmation	**Date**

* Sole Source must include Certificate of Exemption
**Project Description not required for Sole Source

FOR SMBR USE ONLY			
Date Received		Date Assigned to BDC	
In accordance with Chapter2-9(A-D)-19 of the Austin City Code, SMBR makes the following determination:			
☐ Goals	% MBE		% WBE
☐ Subgoals	% African American		% Hispanic

City of Austin
SMBR
Small & Minority Business Resources
Opening the door to opportunities

	% Asian/Native American	% WBE
☐ Exempt from MBE/WBE Procurement Program	☒ No Goals	

This determination is based upon the following:

☐ Insufficient availability of M/WBEs   ☐ No availability of M/WBEs
☒ Insufficient subcontracting opportunities   ☐ No subcontracting opportunities
☐ Sufficient availability of M/WBEs   ☐ Sufficient subcontracting opportunities
☐ Sole Source   ☐ Other

If Other was selected, provide reasoning:

MBE/WBE/DBE Availability

There are 25 MBEs and 10 WBEs available to bid as primes.

Subcontracting Opportunities Identified

There are no subcontracting opportunities identifed. This solicitation requires a software solution (20811) that includes implementation of software and ongoing maintenance of said solution (92045). It would be difficult to separate out functions to use subcontractors if the prime has to create the software and maintain it. Subcontractors would not be able to grasp the software as it is likely to be unique to the prime.

Sonya Powell		
SMBR Staff Sonya Powell	**Signature/ Date** 10/30/18	
SMBR Director or Designee	**Date** 10/31/18	
Returned to/ Date:		