



Independent Review

For the

Managing Assets for Transportation (MATS)
Contract Amendment for Level Funding and Support
State of Vermont
Department of Transportation

Submitted to the
State of Vermont, Office of the CIO

By

Mr. Bob Carroll, Senior Consultant, Independent Reviewer
Mr. Daniel McLane, Senior Partner, PMP, Project Manager
Mr. Mark Peterson, Managing Partner, Quality Assurance

Coeur Business Group, Inc.
18 Hawk Ridge Blvd. suite 200
Lake Saint Louis, MO 63367
800-335-9029

July 5, 2013

Table of Contents

MANAGING ASSETS FOR TRANSPORTATION (MATS)	1
1.0 EXECUTIVE SUMMARY	4
RISK SUMMARY	6
INDEPENDENT REVIEW RECOMMENDATIONS	8
<i>IR Disposition of Risk Considering Final Submissions</i>	9
<i>Intended Audience for the Independent Review</i>	9
SUMMARY OF KEY ISSUES	10
PARTICIPANT ACKNOWLEDGEMENT	11
2.0 OVERVIEW OF THIS DOCUMENT AND BACKGROUND	12
SCOPE AND AUTHORITY OF THIS INDEPENDENT REVIEW	12
<i>Authority</i>	12
<i>Scope</i>	12
AOT-MATS PROJECT HISTORICAL BACKGROUND	13
GOALS FOR THE TRI-STATE PARTNERSHIP	14
<i>MATS Contract, Approach, and Business Relationship</i>	14
<i>The MATS Application, Functions, and Successes</i>	15
<i>MATS Primary Functions:</i>	15
<i>MATS Success to Date:</i>	15
REVIEW APPROACH	16
<i>Scope and Context of Independent Review</i>	16
<i>MATS Issues Analysis and Risk Assessment</i>	17
<i>Risk Identification</i>	18
<i>Vermont Policies</i>	19
RISK EVALUATION METHODOLOGY	20
<i>Potential Risk Number</i>	20
<i>Risk Identification to Best Action Mitigation</i>	21
<i>Risk Action Register and Tracking</i>	22
3.0 ACQUISITION COST ASSESSMENT	23
LIMITATIONS OF COST SUMMARY	23
INDEPENDENT REVIEW FINDINGS	23
4.0 TECHNICAL ARCHITECTURE REVIEW	24
INDEPENDENT REVIEW FINDINGS	24
5.0 ASSESSMENT OF IMPLEMENTATION PLAN	25
THE REALITY OF THE TIMETABLE	25
ADEQUACY OF THE VENDOR’S PROPOSED RISK MANAGEMENT PLAN	26
ADEQUACY OF DESIGN, CONVERSION, AND IMPLEMENTATION PLANS	26
ADEQUACY OF SUPPORT FOR CONVERSION AND IMPLEMENTATION ACTIVITIES	26
ADEQUACY OF THE VENDOR’S TRAINING PLAN	26
ADEQUACY OF PLANNED TESTING PROCEDURES	26
INDEPENDENT REVIEW FINDINGS	27
6.0 ASSESSMENT OF ORGANIZATIONAL READINESS	27
GENERAL PROJECT ACCEPTANCE / READINESS OF STAFF	27
<i>State Staffing</i>	27
<i>Vendor Staffing</i>	27
INDEPENDENT REVIEW FINDINGS	28
7.0 COST BENEFIT ANALYSIS	29

COSTS	29
BENEFITS	30
<i>Goals for the Tri-State Partnership</i>	30
<i>The MATS Application, Functions, and Successes</i>	30
<i>MATS Primary Functions:</i>	30
<i>MATS Success to Date:</i>	31
8.0 RISKS AND ISSUES MANAGEMENT PLAN	32
DEFINITIONS: FINDINGS, RISKS, ISSUES	32
ISSUES AND POTENTIAL RISKS	32
HIGH RISK ITEMS – REMEDIATION AND MITIGATION REQUIRED	33
INDEPENDENT REVIEW RISK REGISTER	34
REMAINING RISK DISCUSSION AND EXPLANATION	36
<i>Compliance with existing Vermont Information Technology policies</i>	36
<i>Compliance with Procurement and acquisition Policy</i>	36
<i>Continuity of Operations (COOP) and Disaster Recovery</i>	37
<i>Structured Processes and methodologies with documentation</i>	37
<i>MATS and Business Alignment with respect to VT IT Strategic Plan</i>	
<i>Principles for the period 2013-2018</i>	38
<i>MATS Information Security</i>	38
<i>(MATS) Program and Portfolio Management (PPM)</i>	39
<i>(MATS) Contract and Support</i>	39
DETAILED RISK “BEST ACTIONS” FOR REMEDIATION	40
<i>Strategy and Funding Risks</i>	40
<i>Architecture and Technology Risks</i>	41
<i>Human Capital Management Risks</i>	41
<i>Tools and Processes Risks</i>	42
<i>Data Management Risks</i>	42
<i>Governance Risk, and Compliance Risks</i>	43
BEST ACTIONS FOR REMEDIATION FOR INTERIM OPEN ITEMS (AS OF 7/01/2013)	44
SUMMARY	45
<i>Key Cost Impact Issue:</i>	45
FINAL RISK DISPOSITION (AS OF 8/01/2013)	47
	49
APPENDIX A – PROJECT COST DETAILS	50
APPENDIX B – ORIGINAL RISKS SUMMARY	51
<i>Risk Details by Domain All Scores</i>	51
<i>Strategy and Funding</i>	51
<i>Architecture and Technology</i>	52
<i>Human Capital Management</i>	52
<i>Tools and Processes</i>	53
<i>Data Management</i>	53
<i>Governance Risk, and Compliance</i>	54
APPENDIX C – DELCAN STATEMENT OF WORK (TASKS)	55
APPENDIX D – INITIAL RISK STRATEGY AND SUBMISSIONS	62
APPENDIX D – PROJECT COSTS TO DATE	70

1.0 Executive Summary

The State of Vermont's Department of Information and Innovation (DII) engaged Coeur Business Group, Inc. (Coeur Group) to conduct an Independent Review of the continuing AOT-MATS project.

Coeur Group initially identified key stakeholders and scheduled individual interviews and work sessions with staff and management from the Vermont Agency of Transportation (AOT) as well as the Department of Transportation personnel from the state of New Hampshire and the state of Maine who are also co-participants in the AOT-MATS project.

Coeur Group interview staff and management from the Department of Information and Innovation (DII) with regards to the AOT-MATS project management capabilities and interaction with the DII EPMO.

The state's AOT – MATS IT manager provided Coeur Group with additional documents that were used to conduct this review. In addition the tri-state program manager coordinated activities and schedules as well as providing additional material to conduct this review.

Additional documents provided included;

- Sole-source justification for MATS 2012
- MATS tri-state partnership
- MATS architecture revised documentation
- MATS presentation IHEEP Dearborn 2010
- MATS time and labor presentation
- Sole-source contract with Delcan Statement of Work
- Tri-state memo of understanding (MOU) November 2004 final
- Vermont MD collaborative agreement revised draft 9222011
- AOT procedures for contract services – scanned 20130221
- MATS AA14 and documentation 20130221
- MATS requirements VT DWR 1
- VT PS 0007 task 14 VT payroll implementation
- VT PS 0007 task 15 MP general enhancements

State of Vermont statute requires the DII to solicit an Independent Review for all information technology projects estimated to exceed \$500,000. In this case, the Independent Review examined the Sole Source selection process for the Vermont Agency of Transportation Managing Asset for Transportation (AOT-MATS) project.

The State Office of the Chief Information Officer (CIO) sought an independent assessment of the State's selected sole source vendor, Delcan and its extension of the existing contract for the next 4 years regarding proposed costs, the architecture of the proposed solution, the vendor's proposed implementation

plan, and the vendor's capacity to provide the proposed equipment, support, and services over the next 4 year period.

The primary objective of the Independent Review is to identify risks and issues that may impact the success of the project.

The primary entities involved in this Independent Review include, but are not limited to:

- Delcan the current MATS vendor
- Vermont Department of Transportation (VTrans)
- Department of Information and Innovation (DII) EPMO and Chief Information Officer
- New Hampshire Department of Transportation
- Maine Department of Transportation

This Independent Review (IR) was conducted on the Vermont Agency of Transportation (VTrans) – MATS (Managing Assets for Transportation) system for the Department of Information and Innovation (DII) as required by Vermont Statute, Title 3, Chapter 45, §2222(g). The VTrans – MATS system has been in existence for roughly 16 years and this IR is specific to the next four-year funded extension of the program starting in 2013 as required by this statute. MATS, is a combined effort between the State of Vermont, New Hampshire and Maine. Future additions may include the State of Maryland and potentially Michigan.

For this IR, Information was collected via various means including individual interviews with personnel from all three of the member states. Critical Success Factors for this project were identified from each of the participants interviewed. These Critical Success Factors along with current and future risks were identified, documented and prioritized. The independent reviewer (Coeur Group) identified, quantified, and captured the risk in a "Risk Action Register" providing each risk with a Potential Risk Number (PRN) to define the Potential of the risk, Severity of the risk and the Detectability of the risk.

Based upon discussions and review meetings the Independent Reviewer provided recommendations. The implementer (VTrans) working with DII, then formulated a plan and addressed those risk(s).

To determine risk, Coeur Group collected and compared artifacts and observations to the applicable standards and controls. In this case, that is the State of Vermont's Department of Information and Innovation (DII) policies and procedures for independent reviews.

The risks were identified in six categorical areas including:

1. Strategy And Funding
2. Architecture And Technology
3. Human Capital Management
4. Tools And Processes
5. Data Management
6. Governance Risk And Compliance

Risk Summary

In total 29 risks were identified and documented with specific recommendations by Coeur Group for remediation.

These risks were identified during the initial interviews and analysis of the past AOT-MATS program as well as current and future plans by AOT and the three participating states. The following table shows the 29 risks identified during the discovery phase of the Independent review.

Risk Category	Identified Risk
Strategy and Funding	Non-alignment of MATS [legacy project] with 6 points for 2013 in 5 year plan for IT from DII
	Currently, the MATS application is sole –sourced relying on DELCAN only
	MATS is developed using discrete 'Tasks' with limited consideration to an overall Roadmap. The last update was 2009
	There does not appear to be a local documented SDLC for VT including development and user acceptance testing with respect to configuration and customization, support, maintenance.
	VTrans uses MATS for Time and Billing. The rest of VT will be using Vision
	Many users will use Citrix to access MATS in VT in the event of an emergency or security event
	It was reported that DII could be taking over MATS support for servers, then application. "DII doesn't understand application"
Architecture and Technology	MATS uses a thick client interface. This architecture is platform specific, and results high total cost of ownership
	There is little virtualization in use currently with MATS in VT
	Lack of enforcement by code for password policies. This should include access logs for MATS
	STARS finance is being replaced by Vision in the next

	month
Human Capital Management	Within Vermont, MATS knowledge is concentrated among a few individuals. In some case this is one or 2 individuals
	Currently, there is no structured MATS training program
	The COOP plan has not been tested
	Currently, DII is not equipped to support the 7x24x365 requirements of MATS
Tools & Process	There is little to no process documentation with MATS processes
	Client/server approach is not best practice, platform specific, and high total cost of ownership
	There is no on-line 'Help'
	MATS issue reporting and release management is migrating to a new system
	The pre-configured reports are not flexible enough for end users.
	Testing and User Acceptance Testing is performed in Delcan environment
	Support and Maintenance is Task based and only for 14 days after delivery and acceptance.
	Existing documentation does not follow any accepted standards (ISO)
Data Management	
	With respect to Vision ERP, the data exchange file format is in flux and not defined. This issue is not unique to MATS and is indicative of a bigger issue and lack of a Master Data Model within the SoV
Governance, Risk, and Compliance	
	Non-Compliance with Information Resource Management Advisory Council Five-Year Plan for Information Technology
	Non-Compliance with Information Resource Management Advisory Council Cost Benefit Analysis
	Lack of current and up-to-date COOP and/or D/R Plan
	Lack of 5 year Maintenance and support plan
	Currently, there is a lack of Key Performance Indicators and measurement criteria with respect to MATS and MATS OPS.
	Non-compliance with source code requirements with respect to the State of Vermont (possession)
	Lack of compliance with respect to DII Security Standards policy
	Information Security - Pentest and Vulnerability Scan being performed by AOT and Delcan.
	Lack of Independent Review for each TASK/SOW

During this independent review, AOT was very diligent and worked collaboratively to correct the risks and mitigation of the identified risk.

Inasmuch as some of the identified risk will require additional effort and time to implement remediation, there are still six (6) outstanding risk items as of this writing that require completion and closure between AOT and DII.

The continued implementation of the proposed solution carries with it potential risks to the State in the following areas which include:

1. Lack of enforcement by code for password policies.
2. Testing and User Acceptance Testing is performed in Delcan environment
3. Support and Maintenance is “Task” based and only guaranteed for 14 days after delivery and acceptance.
4. Lack of current and up-to-date COOP and/or D/R Plan
5. Lack of compliance with respect to DII Security Standards policy
6. Lack of Independent Review for each TASK/SOW

Independent Review Recommendations

Coeur Group recommends that DII proceed with approving 2013-2017 contract with the following noted conditions/actions to be completed based upon an agreed upon schedule with the Department of Information and Innovation (DII):

1. DII/VTrans address each of the **RED** and **YELLOW** risks Best Actions in Risk Discussion section of the IR.
2. MATS and (MATS functionality i.e. time entry, work orders, asset management, planning and budgeting) should be included in Vermont State Project and Portfolio Management.
3. Perform a **Risk Assessment** for MATS as soon as practical.
4. Update and TEST the Continuity of Operations Plan (COOP) and Disaster Recovery Planning for MATS. This should be documented and tested with auditable results capability.
5. MATS support and Human Capital should be leveraged and follow SoV guidelines, lessons learned and recommended practices from Vantage and Vision projects.
6. A project review by DII and VTrans should be conducted at each funding milestone or alternately an entire project scope for the total allocated funds.

IR Disposition of Risk Considering Final Submissions

As described later in this report, the disposition of the risk items listed below will need to be acted upon and brought to closure between DII and AOT.

Each of the following six (6) Risk items are still open and require action for closure and include:

1. Lack of enforcement by code for password policies.
2. Testing and User Acceptance Testing is performed in Delcan environment
3. Support and Maintenance is Task based and only for 14 days after delivery and acceptance.
4. Lack of current and up-to-date COOP and/or D/R Plan
5. Lack of compliance with respect to DII Security Standards policy
6. Lack of Independent Review for each TASK/SOW

Intended Audience for the Independent Review

This independent review is intended for public review as well as utilization within the state of Vermont and in particular the Department of information and innovation and the Vermont Agency of Transportation (AOT). It is anticipated that the following audience would be the potential viewers of this document and include;

- Members of the public through the Freedom of Information Act – FOI
- DII – Office of the CIO
- VTrans (Agency of Transportation - AOT)

Summary of Key Issues

Key issues are different from the risk ranking and prioritization of issues. With respect to the PRN Potential Risk Number, many of the issues do have controls or remediation in place, therefor are being addressed in this summary.

The key issues identified are shown in the following table:

Key Issue	Independent Review Indication(s)
(Lack of) Compliance with existing Vermont Information Technology related policies and statutes.	<ul style="list-style-type: none"> • Independent Review (now in compliance) Policy • 5 year plan Policy • Security Policy
Continuity of Operations (COOP) and Disaster Recovery for a <u>CRITICAL SYSTEM</u>.	Current plan is not up to date or tested. COOP plan needs to address a Risk Assessment for MATS. To date a formal Risk Assessment has not been performed on MATS
MATS and Business Alignment with respect to VT IT Strategic Plan 2013-2018	MATS is not fully aligned with the 6 IT Strategic principles for 2013 work (SoV IT Strategic Plan 2013-2018)
Program and Portfolio Management (PPM) as it pertains to MATS Tasks(SOW)	(Lack of) Strategic planning for MATS and MATS functionality at the State level. Currently, there are 2 systems for time entry. Multiple systems for asset tracking and work order management in SoV.
Lack of structured processes and methodologies with documentation	MATS supporting processes and methods have minimal documentation, artifacts, scripts or auditable proof of compliance with controls. This was an issue with the IR.
MATS Information Security	Could not locate a Risk Assessment of MATS application. (start of security plan) Scans performed by Delcan and VTrans. (need to be 3 rd party)
Unconventional (MATS) Contract and Support	To date the contract and support is sole-sourced, lacks maintenance or support, and Tasks (i.e. SOW) are not subject to IR process.

COEUR POINT: Based on the Independent Review and identified risks, Coeur Group recommends that DII ***Proceed with approving 2013-2017 contract*** for AOT-MATS with the following noted conditions/actions in this report to be completed based upon an agreed upon schedule with the Department of Information and Innovation (DII) and AOT.

Participant Acknowledgement

Coeur Group wants to thank the parties aiding in this Independent Review (IR) for their time and effort to enable a complete review of the VTRANS-MATS current state and planned next four (4) year time period. Especially those who took time to be interviewed and provide additional information and data including:

Name	Title
Betsy Ross-Mobbs	Information Technology-Manager III - VTrans
Wayne Gammell	Maintenance Transp. Administrator - VTrans
Alec Portalupi	Technical Service Engineer - VTrans
Amy Mercier	Operations Administrator - VTrans
Robert T. White	Tri-State Program Manager - VTrans
Chris Zebrowski	Technical Lead - Delcan
Randy Geaumont	Maintenance and Operations, ME DOT
Andy Bickmore	Division Director – ME DOT
Bill Watson	Administrator MATS Project Manager – NH DOT
John Clarke	Information Technology MATS User Support – NH DOT
Nick Alexander	MATS Project Manager – NH DOT
Martha Haley	Vermont DII EPMO – Project Manager

Regards,

Robert Carroll
 Independent Reviewer
 Coeur Business Group, Inc.

Mark A. Peterson
 Managing Partner
 Coeur Business Group, Inc.



2.0 Overview of this Document and Background

Scope and Authority of this Independent Review

Authority

The scope of this document is fulfilling the requirements of Vermont Statute, Title 3, Chapter 45, §2222(g):

“The secretary of administration shall obtain independent expert review of any recommendation for any information technology activity initiated after July 1, 1996, as information technology activity is defined by subdivision (a)(10) of this section, when its total cost is \$500,000 or greater. Documentation of such independent review shall be included when plans are submitted for review pursuant to subdivisions (a) (9) and (10) of this section. The independent review shall include:

- (1) an acquisition cost assessment;*
- (2) a technology architecture review;*
- (3) an implementation plan assessment;*
- (4) a cost analysis and model for benefit analysis; and*
- (5) a procurement negotiation advisory services contract.”*

Scope

The scope of this review involves the **amendment and contract extension** of the AOT-MATS program which has been in progress for the past 8 years. This IR was focused on the next segment of the program which entails the next 4 year period.

- Tri-State Program Contract PS0007 Task 14
- Tri-State Program Contract PS0007 Task 15

On or about, April 10-12 a series of interviews were conducted in person and by phone with the following individuals using Coeur Group’s Independent Review interview template as a framework.

Name	Role/Responsibility	email
Betsy Ross-Mobbs	IT-Manager III - MATS	Betsy.Ross-Mobbs@state.vt.us
Wayne Gammell		Wayne.Gammell@state.vt.us
Alec Portalupi		alec.portalupi@state.vt.us
Amy Mercier	Business Manager	
Robert T. White		

Chris Zebrowski	DELCAN Account and PM	c.zebrowski@delcan.com
Randy Geaumont		Randy.Geaumont@maine.gov
Andy Bickmore		Andrew.Bickmore@maine.gov
Bill Watson		<u>BWatson@dot.state.nh.us</u>
John Clarke		JClarke@dot.state.nh.us
Bill Janelle		BJanelle@dot.state.nh.us

AOT-MATS Project Historical Background

The MATS system – (now Managing Assets for Transportation) has been implemented in Vermont since 1997. The application is also in use in Maine and New Hampshire as part of the Tri-State Program/Partnership formed in 2001 which was expanded in 2004.

The original MATS system in a contract with Booz Allen Hamilton for ~\$500,000 resulted culminated in system that was unusable and unworkable. Following that experience, the parties issued one or more Requests for Proposals to which there was no response by the marketplace. At the time the parties continued their conversation(s) and approached Delcan as a system developer which resulted in a contract and the initial release of MATS.

For the past eleven years the Tri-State Partnership for Maintenance Management among the Vermont Agency of Transportation (VTRANS), New Hampshire Department of Transportation (NH DOT), and Maine Department of Transportation (MEDOT) has been uniquely successful in using the Managing Assets for Transportation System (MATS), as a means of meeting common and shared needs.

MATS has been implemented in Vermont since 1997 and operates in approximately 450 locations supporting over 1300 users.

During the past four years the states have shared a single support contract, administered by VTrans and used (funded) by all three states, to share and leverage software functionality, system enhancements, and upgrades under the basic tenet that capabilities developed by one state will be shared with the other two Partners.

The most recent (3/2009 -> 1/2013) period of the contract for \$4M that server all three partner states and was administered by VTrans produced the following functionality for MATS:

1. VT Payroll
2. ME Asset Modifications Buildings

3. NH User Enhancements and Planning and Budgeting
4. VT Payroll Import
5. VT P&B Support
6. NH Vehicle Legislation
7. ME Performance Measures
8. VT MATS Extensions
9. NH Training
10. MATS CTA Extension
11. Maine Contractor DWR
12. ME Candidate Project Repository
13. VT Payroll Preparation

Goals for the Tri-State Partnership

At that time, the fundamental drivers of the Partnership was the use of a common transportation maintenance and management system to:

- Improve business knowledge and thereby performance
- Support data collection, reporting and tracking
- Automate and improve workflow and processes
- Continually be refined and improved – a living application.

MATS Contract, Approach, and Business Relationship

It should be noted that a somewhat unconventional contracting approach has and will be used with respect to this sole-sourced contract and procurement. During the Independent Review, The team has been given to understand the following:

- VTrans has the sole source contract with the vendor Delcan
- Maine and New Hampshire contribute and reimburse Vermont for features and functionality based on their specific requirements. This roughly works out to one third each.
- New functionality and enhancements are proposed quarterly, or semi-annually to the Tri-State Partnership
- Consensus is reached, and the proposal is completed and turned into a formal Task/Statement of Work submitted to Delcan
- Delcan responds with a Task Order Response included dates and cost.
- The response is accepted by the authorizing authority for VTrans
- The cost for the accepted Task Order Response is deducted from the MATS support contract.
- For the prior contract allocation \$4M, only \$2.7M was actually used.

The MATS Application, Functions, and Successes

MATS Application

Over the past 16 years, through steady enhancement and improvements the MATS application has become the backbone for VTrans. This has led to the improvements and successes as described below.

By design and intent, MATS now has by-and-large replaced manual paper based methods as described in the primary functions section below. As such, the MATS system and application is now designated a **CRITICAL SYSTEM**. This designation as a **Critical System** has special and unique meaning with respect to Vermont State functional impact, continuity of operations, and potentially funding. In common terms, applications and systems with this designation are evaluated with more rigor and held to a higher standard based on the potential impact in the event of an incident or emergency.

MATS Primary Functions:

- Generate Daily Work Report
- Track Central Garage Equipment
- Track Central Garage Equipment Meter Readings
- Track Material Usage
- Provide Feeds for Data System Interfaces
- Materials Management
- Planning & Budgeting
- Manage Maintenance Rental Agreements
- Electronic Asset Management
- Manage Work Orders / Request
- Provide Reports – Timely & Accurate
- Track and Manage Employee Development Tracking

MATS Success to Date:

- Supports 1285 employees in 218 location
- 13 Successful Tasks completed to date
- Feed data to VT Payroll
- VT Payroll Import and Sync
- VT Planning & Budgeting Support
- VT MATS Extensions
- VT MATS Rental Agreements
- MATS CTA Extension
- VT Payroll Preparation
- Reduction in paper usage

- More accurate information available on demand
 - Billing for hurricane Irene
 - FEMA (Federal Emergency Management Agency) grants resulting in \$70M to VT for hurricane Irene relief supported by MATS data
 - FWHA (Federal Highway) Administration relief for Irene
- Elimination of duplicate time entry

Review Approach

Coeur Group’s approach for this independent review includes the following:

- Identification of all key stakeholders
- Individual and group interviews with all key stakeholders from three states including New Hampshire, Maine and Vermont
- Review of all provided material for cost, benefit, architecture and infrastructure for the AOT – MATS
- Review of past and future plans for continued implementation of the AOT – M ATS system
- Validation sessions with DII and VTrans personnel
- Documentation of individual risk items in the risk action register

Scope and Context of Independent Review

It should be noted that the scope of this review involves the Delcan Sole Source contract and amendment and contract extension provided to Coeur Group using the suggested template furnished by DII as a baseline of review framework.

Other touch points and considerations are how the MATS roadmap and futures (where possible) relate to the wise use of Vermont resources, current laws and statutory requirements, and current and future IT strategy.

The period of this contract is 2013 -> 2017.

It is NOT within scope of the IR to evaluate MATS as an application and system in its entirety since it has been in continuous development since 1997.

MATS Issues Analysis and Risk Assessment

The following criteria were used with respect to the risk evaluation. **For purposes of this Independent Review (IR), if the item or artifact isn't in writing, or current – up-to-date it is identified as a deficiency and/or non-compliance.** Hence responses like 'We do X', or 'We have that' are and were not considered without proof or evidence, usually in writing. This is most commonplace with respect to processes, procedures, testing, and audit trails.

For the Independent Review, where Vermont State statutes, methodologies, policies, or procedures do not exist, or have gaps - usual normal and customary industry standards and methodologies will be used from the partial list below in the table.

Coeur Consultants utilize standards for Maturity Models and testing tools as indicated below:

<i>Practice Area</i>	<i>Standard/Reference</i>	<i>Name/Subject</i>
Project Management	IEEE 1490-2003 PMI PMBOK	Adoption of Project Management Institute (PMI) Standard
Software Project Management	IEEE 1058-1998 IEEE 12207-2008	S/W Project Management Plan (SPMP) Information Technology – Software life cycle processes
IT/Software Design and Development	IEEE 1063-2001 IEEE 1471-2000 IEEE 2001-1999	Standard for S/W User Documentation Recommended Practice for Architectural Description (AD) of S/W Intensive Systems Recommended Practice for Intranet Practices – Web Page Engineering – Intranet/Extranet Applications
Work Breakdown Structure	PMI Practice Standard	PMI Practice Standard for Work Breakdown Structure (WBS)
Risk Management	ISO/IEC 16085-2006	Risk Management
Requirements Management	IEEE 830-1998 IEEE 1233-1998	Recommended Practice for S/W Requirements Specification Guide for Developing System Requirements Specifications (SyRS)
Configuration Management	IEEE Std 828-2005	S/W Configuration Management
Quality Management	IEEE 730-2002 IEEE 1012-2004 IEEE 1028-2008 IEEE 1061-1998	Quality Assurance Plan S/W Verification and Validation Standard for Software Reviews and Audits Quality Metrics Methodology
Test Strategy & Plans	IEEE 829-1998	Standard for Test Documentation

	IEEE 1008-1987	Software Unit Testing
S/W Maintenance and Operations	IEEE Std 14764-2006	Software Engineering — Software Life Cycle Processes — Maintenance

Coeur Consultants utilize standards for Information Security – NIST (National Institute of Standards and Technology) IT Security as listed below:

SP 800-123	Guide to General Server Security
SP 800-116	A Recommendation for the Use of PIV Credentials in Physical Access Control Systems (PACS)
SP 800-114	User’s Guide to Securing External Devices for Telework and Remote Access
SP 800-111	Guide to Storage Encryption Technologies for End User Devices
SP 800-100	Information Security Handbook: A Guide for Managers
SP 800-95	Guide to Secure Web Services
SP 800-88	Guidelines for Media Sanitization
SP 800-64 Rev 2	Security Considerations in the Information System Development Life Cycle
SP 800-63 Rev 1	Electronic Authentication Guideline
SP 800-53 Rev 3	Recommended Security Controls for Federal Information Systems and Organizations
SP 800-48-1	Guide to Securing Legacy IEEE 802.11 Wireless Networks
SP 800-47	Security Guide for Interconnecting Information Technology Systems
SP 800-44-2	Guidelines on Securing Public Web Servers
SP 800-33	Underlying Technical Models for Information Technology Security
SP 800-27 Rev A	Engineering Principles for Information Technology Security (A Baseline for Achieving Security)
SP 800-14	Generally Accepted Principles and Practices for Securing Information Technology Systems
SP 800-12	An Introduction to Computer Security: The NIST Handbook
NIST IR 7435	The Common Vulnerability Scoring System (CVSS) and its Applicability to Federal Agency Systems
NIST IR 7359	Information Security Guide For Government Executives
NIST IR 7358	Program Review for Information Security Management Assistance (PRISMA)
NIST IR 7298	Glossary of Key Information Security Terms

Risk Identification

Identification of [Project] Risks is a paramount step in the overall IR process for the MATS project. Coeur Group conducted the assessment of project efforts including a detailed review and identification of risks to make recommendations related to policy and processes in areas such as:

• Scope creep	• Schedule acceleration
• Schedule delays	• Ineffective communication
• Inadequate funding	• Momentum loss
• Lack of resources	• Inadequate skills
• Insufficient capacity	• Loss of sponsorship
• Requirements shift	• Legislative change
• Ineffective project governance	• Ineffective training

<ul style="list-style-type: none"> • User resistance to change 	<ul style="list-style-type: none"> • Over reliance on vendor resources
<ul style="list-style-type: none"> • Loss of data integrity 	<ul style="list-style-type: none"> • Regulatory non-compliance

Vermont Policies

Also whereby Vermont has a number of Vermont State policies that affect Information Technology projects, the following Vermont specific items were also used in the Independent Review:

- *The State’s Information Technology Policies & Procedures at: http://dii.vermont.gov/Policy_Central*
- *The State’s Record Management Best Practice at: <http://vermont-archives.org/records/standards/pdf/RecordsManagementBestPractice.pdf>*
- *The State Information Security Best Practice Guideline at: [http://vermont-archives.org/records/standards/pdf/InformationSecurityBestPractice Eff.20090501.pdf](http://vermont-archives.org/records/standards/pdf/InformationSecurityBestPracticeEff.20090501.pdf)*
- *The State Digital Imaging Guidelines at <http://vermont-archives.org/records/standards/pdf/ImagingGuideline2008.pdf>*
- *The State File Formats Best Practice at [http://vermont-archives.org/records/standards/pdf/FileFormatsBestPractice Eff.20071201.pdf](http://vermont-archives.org/records/standards/pdf/FileFormatsBestPractice_Eff.20071201.pdf)*
- *The State File Formats Guideline at <http://vermont-archives.org/records/standards/pdf/FileFormatsGuideline2008.pdf>*
- *The State Metadata Guideline at <http://vermont-archives.org/records/standards/pdf/MetadataGuideline2008.pdf>*

Risk Evaluation Methodology

Coeur Group utilizes a **Risk Assessment and Action Register** to track all project risk and best actions to resolve the risk. Each Risk is assessed and weighted as to **Risk Severity, Risk Probability and Risk Predictability**.

Potential Risk Number

Coeur Group assesses Risk in three distinct categories. The Risk rankings are defined in a scale of 1 to 10, these are shown in the chart below and include;

Severity of the Risk Event: This identifies the relative **SEVERITY** of the risk event.

Probability of the Risk Event: Determining the **PROBABILITY** of a risk event is critical and enables proper planning for risk reduction.

Current Controls of Risk: This identifies the capability to **DETECT** a risk event.

Severity of Event (S)	Ranking	Probability of Event (P)	Ranking	Current Controls C (Detection)	Ranking	
Hazardous: Without warning	10	Very High: Event is almost inevitable	10	Absolute uncertainty	10	Low Controls
Hazardous with warning	9		9	Very Remote	9	
Very high	8	High: Repeated Events	8	Remote	8	
High	7		7	Very Low	7	
Moderate	6	Moderate: Occasional events	6	Low	6	
Low	5		5	Moderate	5	
Very Low	4		4	Moderately High	4	
Minor	3	Low: Relatively Few Events	3	High	3	
Very Minor	2		2	Very High	2	
none	1	Remote: Event is Unlikely	1	Almost Certain	1	High Controls

Based on the evaluators score and ranking in each of the domains; Severity, Probability, and Controls/Detections an arithmetic score is generated resulting in the **Potential Risk Number** or **PRN**. With a PRN score, the risks can then be sorted and prioritized.

Risk Identification to Best Action Mitigation

Each Risk or Issue is then entered into the Coeur Group “Risk Action Register”. The risk item or functional issue is identified in one of five risk domains which include;

- Strategy And Funding,
- Architecture And Technology,
- Human Capital Management,
- Tools And Processes,
- Data Management,
- Governance, Risk and Compliance

ID	Item/Function Issue	Potential Risk Event	Severity of Event	S	Probability of Event	P	Current Controls (Detection)	C	PRN	Best Actions
Strategy and Funding										
S1	Non-alignment of MATS [legacy project] with 6 points for 2013 in 5 year plan for IT from DII	Not optimal or collaborative strategy		3		10		1	30	Meeting of parties and reconcile
S2	Currently, the MATS application is sole-sourced relying on DELCAN only	Custom developed solutions present a risk due to lack of industry standards and proprietary nature of solution		5		6		5	150	Develop contingency plan and examine COTS software
S3	MATS is developed using discrete 'Tasks' with limited consideration to an overall Roadmap. The last update was 2009	Lack of 'big picture' and shifts in technology and trends		5		10		3	150	Update 2009 Roadmap with concerned parties
S4	There does not appear to be a local documented SDLC for VT including development and user acceptance testing with respect to configuration and customization, support, maint.	Bugs, problems and failures due to adequate testing and acceptance		4		8		3	96	Document and implement testing, acceptance, roll-out and support plan
S5	Vtrans uses MATS for Time and Billing. The rest of VT will be using Vision			3		10		2	60	This issue needs to be reconciled. According to VTrans, there is a Fed. Reporting requirement that Vision is incapable of supporting
S6	Many users will use Citrix to access MATS in VT in the event of an emergency or security event	Citrix is supported by DII. If Citrix goes down, MATS will be unusable		10		6		8	480	Evaluate Citrix Risk and contingency plans. MATS/Vtrans need s to conduct a Risk Assessment That includes Citrix
S7	It was reported that DII could be taking over MATS support for servers, then application. "DII doesn't understand application"	Lack of support, and mistakes (at least 2 incidents to date). One resulting in MATS being down for 3 days		9		6		4	216	Develop strategy and plan with respect to Human Capital, IT and business alignment

Risk Prioritization and Best Action Statement

Once the risk item is described, a potential risk event is identified. Once the risk event is identified a potential risk number is developed by determining the severity of the event, the probability of the event and the detectability with current controls of the event. These numerically derived a potential risk number or PRN.

Based upon the discussions and risk events, a best action is recommended for mitigation or risk reduction. This best action is documented in the Risk Action Register.

Risk Action Register and Tracking

The Risk Action Register is an Excel Spreadsheet and has multiple Tabs. The next Tab provides further action tracking by defining the Staff owner; the Task person assigned the action, the entry date, the finish date, the target completion date, a secondary assignable priority (high-medium-low). The Action Register provides date tracking to enable easy visual tracking of assigned tasks.

Required		Optional (But recommended)					Calculated			
Item/Function Issue	Best Action	Staff Owner's Name	Task Person Name	Entry Date	Finish Date	Target Date	High = Red Med = Yellow Low = Green	PRN Priority	Status CLOSED / OPEN	Days 5d / 7d
Strategy and Funding									OPEN	#VALUE!
Non-alignment of MATS [legacy project] with 6 points for 2013 in 5 year plan for IT from DI	Meeting of parties and reconcile						N/A	0		
Currently, the MATS application is sole-sourced relying on DELCAN only	Develop contingency plan and examine COTS software						N/A	30		
MATS is developed using discrete 'Tasks' with limited consideration to an overall Roadmap. The last update was 2009	Update 2009 Roadmap with concerned parties						N/A	150		
There does not appear to be a local documented SDLC for VT including development and user acceptance testing with respect to configuration and customization, support, maint.	Document and implement testing, acceptance, roll-out and support plan						N/A	150		
Vtrans uses MATS for Time and Billing. The rest of VT will be using Vision	This issue needs to be reconciled. According to VTrans, there is a Fed. Reporting requirement that Vision is incapable of supporting						N/A	96		
Many users will use Citrix to access MATS in VT in the event of an emergency or security event	Evaluate Citrix Risk and contingency plans. MATS/Vtrans need s to conduct a Risk Assessment That includes Citrix						N/A	60		
It was reported that DI could be taking over MATS support for servers, then application. "DI doesn't understand application"	Develop strategy and plan with respect to Human Capital, IT and business alignment						N/A	490		
								216		

Risk Action Register Indicates Task Assignment and Tracking

3.0 Acquisition Cost Assessment

Limitations of Cost Summary

Detailed Cost information is contained in Section 7.0 of this report. With the MATS project being implemented since 1997, much of the initial cost benefit analysis information was not available for this review. The focus of this independent review resides largely on current and future (next 4 year segment) risk identified and documented in this report.

This IR has reviewed an amendment to an existing contract of with and extension for \$4 million dollars covering the period of 2013 through 2017. This review is focused on the contract extension and its associated plans and risks.

Furthermore, the Independent Review applies only to the existing Tasks (Tasks 14, 15 as defined in the table below) and detailed in Appendix C. covering the respective documentation for those tasks. Other individual tasks for the contract period were not submitted for this IR as they are defined throughout the 4 year time period.

The MATS application to date has been driven by specific requirements that are submitted as **Tasks**. Each **Task** (Statement of Work) is developed as the implementation process progresses and not in a **fully planned timeline** of events.

These Tasks tend to be feature and functional additions that the MATS constituents want and desire and add value to the product from the user's perspective. Unfortunately, this organic and grass roots development does not place equal weight on non-ROI items – at the user level –like security, application architecture, system and user administration. The result is a system that is client/server (thick client) based, some web enablement/support, highly custom, platform specific, and has minimal (application) security built in and I suspect has a high Total Cost of Ownership (TCO) when all things are considered.

Independent Review Findings

Based on the information available for cost factors, this IR indicates significant risk in cost overrun potential due to the methodology utilized by the vendor Delcan for assigning cost to individual task.

Without a formal Project Implementation Plan, Delcan can produce a Task request at any time for any amount as long as it is within limits of Items in ID 1 and ID 2 in the above table. It is up to VTrans management to ensure that each Task order is validated and checked to review completion to expectations.

Risk exists in this process as there is no formal Project Independent Review of each Task order or completion criteria spelled out for Delcan. It is recommended that DII conduct Independent Reviews of each Task order upon development and again upon completion to ensure a validation of completeness is accomplished.

4.0 Technical Architecture Review

On Friday, April 11, 2013 Coeur Group met with the State Chief Technology Officer (CTO), Mr. Mike Morey and reviewed the MATS system architecture. Where MATS is an existing legacy system that has been used for some time, there were no concerns expressed with respect to the Architecture.

With respect to servers and data centers, we understand that there are ongoing discussions with respect to consolidation and location that the CTO is part of.

Independent Review Findings

Based on the history of this program since 1997, and the current infrastructure installed, this IR does not see any significant risk due to the current and future architecture as defined and described by the AOT – MATS program.

Noted Technology Architecture issues include;

- MATS uses a thick client interface. This architecture is platform specific, and results high total cost of ownership
- There is little virtualization in use currently with MATS in VT
- Lack of enforcement by code for password policies.
 - This should include access logs for MATS

5.0 Assessment of Implementation Plan

The Reality of the Timetable

Due to the Sole Source structure of the agreement with Delcan, the AOT-MATS program is very limited in use of an actual timetable or implementation plan.

The MATS application to date has been driven by specific requirements that are submitted as **Tasks**. Each Task is developed as the implementation process progresses and not in a **fully planned timeline** of events. These Tasks tend to be features and functional additions that the MATS constituents want and desire and add value to the product from the user’s perspective. Unfortunately, this organic and grass roots development does not place equal weight on non-ROI items – at the user level –like security, application architecture, system and user administration. The result is a system that is client/server (thick client) based, some web enablement/support, highly custom, platform specific, and has minimal (application) security built in and I suspect has a high Total Cost of Ownership (TCO) when all things are considered.

Delcan has provided the following list as Current Contract Period 2013 -> 2017 Major Tasks and Deliverables:

ID	Completion	Deliverables Description
1	7/15/2013	Task 14 VT Payroll Implementation. The State of Vermont Agency of Transportation (VVTRANS) is requesting services to coordinate with the changes required by the ERP Implementation
2	6/21/2013	Task 15 General Enhancements and additional Admin. Screen. The State of Maine would like to undertake enhancements to Managing Assets on Transportation Systems (MATS) system. This would involve additional administration screens, stop select list screens from refreshing on receiving the focus, Modifications that improve the State of Maine (MeDOT’s) approval reports and process, modifications the reflect the changes to how MATS is used for work planning, and improvements to the procedure of inactivating assets.

Adequacy of the Vendor's Proposed Risk Management Plan

One of the risk areas identified is the lack of a risk management plan and continuity of operations (COOP) plan.

Adequacy of Design, Conversion, and Implementation Plans

Due to the methodology of using task orders for statements of work on a continuing basis as user request our acknowledged, there are no available detail implementation plans for any of the contract elements for item 14 or item 15. Detail of items 14 and 15 are contained in Appendix C.

Task orders are developed whenever a user desires additional functionality or changes. These task orders will be developed and approved periodically throughout the next four-year period.

Adequacy of Support for Conversion and Implementation Activities

Support for M ATS system has been observed during the month of May where Delcan provided one person on site for implementation and planning for the cut over from mainframe and billing application.

Specifically the Delcan maintenance and support contract defines the support window for 14 days after development and go live of any particular task order.

This area has been highlighted in has been recommended that AOT renegotiate the maintenance and support contract with Delcan

Adequacy of the Vendor's Training Plan

The vendor Delcan has no observed or indicated training plan for system usage.

Adequacy of Planned Testing Procedures

It has been noted that Delcan conducts testing on its own test system

and not in a Vermont or tri-state test environment. This has been identified as one of the ongoing risk.

Independent Review Findings

In the areas of Plan Implementation the IR identified the following deficiencies:

- Non-alignment of MATS [legacy project] with 6 points for 2013 in 5 year plan for IT from DII
- Currently, the MATS application is sole –sourced relying on DELCAN only without any optional backup plan
- MATS is developed using discrete 'Tasks' with limited consideration to an overall Roadmap. The last update was 2009. Potential for unplanned expenses on each task order are high
- There does not appear to be a documented Software Development Life Cycle (SDLC) methodology from Delcan for the MATS system including development and user acceptance testing with respect to configuration and customization, support and maintenance
- VTrans uses MATS for Time and Billing. The rest of VT will be using Vision
- Many users will use Citrix to access MATS in VT in the event of an emergency or security event

6.0 Assessment of Organizational Readiness

General Project Acceptance / Readiness of Staff **State Staffing**

With respect to staffing by the state, the following items have been identified as issues including:

- Within Vermont, MATS knowledge is concentrated among a few individuals. In some case this is one or 2 individuals
- Currently, there is no structured MATS training program
- The COOP plan has not been tested
- Currently, DII is not equipped to support the 7x24x365 requirements of MATS
-

Vendor Staffing

Based on historical support and maintenance of the AOT – mats system, Dell can has been providing sufficient support to the tri-state

program. Based on input from AOT personnel, Dell can is providing sufficient maintenance and support staffing to the tri-state program.

Independent Review Findings

Based on the assessment of organizational readiness the key issues have been highlighted about which include the readme for DI to ready itself to support the mats systems requirements based on an agreed upon Service Level Agreement (SLA).

In addition we have highlighted the fact that only a couple AOT personnel are knowledgeable about the full mats and its functionality. Since this is a tri-state program and will likely include the state of Maryland soon it is imperative that an additional training for system management and users be available from Delcan.

7.0 Cost Benefit Analysis

Costs

With the project being implemented since 1997, much of the initial cost benefit analysis information was not available for this review. The focus of this independent review resides largely on current and future (next 4 year segment) risk identified and documented in this report.

Where this is an amendment to an existing contract, this review is focused on the **contract extension**. Cost since 1997 is beyond the scope of this Independent Review of MATS.

Delcan has provided the following list as Current Contract Period 2013 -> 2017 Major Tasks and Deliverables:

ID	Cost	Completion	Deliverables Description
1	\$245,000 (VT)	7/15/2013	Task 14 VT Payroll Implementation.
2	\$225,000 (ME)	6/21/2013	Task 15 General Enhancements and additional Admin. Screen. To the procedure of inactivating assets.
	\$470,000	Total allocated for Delcan	
	\$4,000,000	Budget/ Contract Total	
	\$3,530,000	NOT allocated as of 4/2013	

Prior Contract Period 2009 -> 2013 Major Tasks and Deliverables

ID	Cost	Year	Vermont Only Amt.	
1	\$1,320,000	2009	\$485,000	
2	\$975,000	2010	\$580,000	
3	\$350,000	2011	\$100,000	
4	0	2012		
	\$2,645,000	Total Spend with Delcan		\$1,165,000 44%*
	\$4,000,000	Budget/ Contract Total		
	\$1,355,000	*Undetermined spend for this IR		

* It should be noted that for the prior contract period, Vermont funded 44% of the total cost. A chart with the historical data is available in the appendix.

Benefits

Although not defined specifically, the Benefits of the Tri-State MATS systems has been the cost savings from utilization of a common Asset Management and Tracking system across three states. Soon the State of Maryland is planning on joining this consortium of Transportation users.

Goals have been stated and the Management seems positive in its gains from utilization of the system.

This Independent Review acknowledges the positive cost savings derived from joint utilization of one system. It is also noted (as shown in the table above) that only 44% of the previous periods funds were utilized for the program.

Goals for the Tri-State Partnership

At the time of program initiation in 1997, the fundamental driver of a Tri-State Partnership was the use of a common transportation maintenance and management system to:

- Improve business knowledge and thereby performance
- Support data collection, reporting and tracking
- Automate and improve workflow and processes
- Continually be refined and improved – a living application.

The MATS Application, Functions, and Successes

MATS Application

Over the past 16 years, through steady enhancement and improvements the MATS application has become the backbone for VTrans. This has led to the improvements and successes as described below.

By design and intent, MATS now has by-and-large replaced manual paper based methods as described in the primary functions section below. As such, the MATS system and application is now designated a **CRITICAL SYSTEM**. This designation as a **Critical System** has special and unique meaning with respect to Vermont State functional impact, continuity of operations, and potentially funding. In common terms, applications and systems with this designation are evaluated with more rigor and held to a higher standard based on the potential impact in the event of an incident or emergency.

MATS Primary Functions:

- Generate Daily Work Report

- Track Central Garage Equipment
- Track Central Garage Equipment Meter Readings
- Track Material Usage
- Provide Feeds for Data System Interfaces
- Materials Management
- Planning & Budgeting
- Manage Maintenance Rental Agreements
- Electronic Asset Management
- Manage Work Orders / Request
- Provide Reports – Timely & Accurate
- Track and Manage Employee Development Tracking

MATS Success to Date:

- Supports 1285 employees in 218 location
- 13 Successful Tasks (Statements of Work) completed to date
- Feed data to VT Payroll
- VT Payroll Import and Sync
- VT Planning & Budgeting Support
- VT MATS Extensions
- VT MATS Rental Agreements
- MATS CTA Extension
- VT Payroll Preparation
- Reduction in paper usage
- More accurate information available on demand
 - Billing for hurricane Irene
 - FEMA (Federal Emergency Management Agency) grants resulting in \$70M to VT for hurricane Irene relief supported by MATS data
 - FWHA (Federal Highway) Administration relief for Irene
- Elimination of duplicate time entry

8.0 Risks and Issues Management Plan

Definitions: Findings, Risks, Issues

The responsibility for corrective action for each identified risk is the role of the implementer Agency/Department (VTrans) to take the specific actions and pursue the recommendations. The mechanism for this has been the **DRAFT IR** report and meeting/review process where the preliminary findings have been shared and in this case VTrans was an active participant and was afforded the opportunity to respond and react to the findings. Those responses are contained herein for the final report.

Issues and Potential Risks

The results of the issues and risk analysis are presented in the spreadsheet below using the Coeur Group methodology outlined in **Risk Evaluation Criteria** on page 20.

For informational purpose the Potential Risk Numbers – PRN are color coded in stop-light format for visual impact and for ease of reading. The legend is as follows:

Potential Risk Number	Color	Definition
PRN Score = 0 to 100	Green	Green – Acceptable Risk
PRN Score = 101 to 350	Yellow	Yellow = Moderate Risk With Monitoring And Controls
PRN Score > 350	Red	Red = High Risk, Remediation And Mitigation Required

High Risk Items – Remediation and Mitigation Required

On April 19, 2013 the DRAFT findings of the MATS IR were shared in a meeting with the following attendees:

- Boes, Richard <Richard.Boes@state.vt.us>;
- Thompson, Darwin <Darwin.Thompson@state.vt.us>;
- Haley, Martha<Martha.Haley@state.vt.us>;
- Ross-Mobbs, Betsy <Betsy.Ross-Mobbs@state.vt.us>;
- Hurd, Tom <Tom.Hurd@state.vt.us>; Hurd, Tom <Tom.Hurd@state.vt.us>;
- Portalupi, Alec <Alec.Portalupi@state.vt.us>;
- Bob.Carroll@coeurgroup.com;

By Phone:

- Mark.Peterson@CoeurGroup.com;
- dan.mclane@coeurgroup.com

In the meeting, it was agreed:

- AOT will review the draft report and provide Coeur Group (cc DII PM) on anything in the report that they feel is incorrect.
- AOT will provide DII with their plan/strategy for addressing each of the red/high risk items in the report. DII PM will confirm with DII CIO that he is on board with these plans/strategies and she will communicate this back to AOT.
- Coeur Group will update his report with these plans/strategies. Coeur Group has some additional work as well to bring the report from a draft to a final version. The report will not be considered final until the CIO signs-off on it.
- AOT will carry out their plans/strategies to address the red/high risk items.
- AOT will notify DII PM when the high risk items have been addressed. DII PM will schedule another meeting with AOT and the CIO to review the completed items. At that meeting, the goal is to obtain CIO approval to enter into the AOT-MATS contract.
- As part of the IR engagement, Coeur Group is also available to provide procurement services. If AOT is interested in having his assistance with the AOT –MATS contract, please let DII PM know by Monday, 4/29

VTrans with DII have been working through these items and next steps and on or about June 21 course of action was determined with respect to the High Risk items the IR will be completed considering the artifacts and latest submissions.

Independent Review Risk Register

Current - -Risk Strategy and Submissions

The following tables reflect the outcomes and actions following the DRAFT review, and additional and revised submissions from VTrans.

The full Risk Register and all items and their associated Potential Risk Number (PRN) are shown on page 35.

In addition, the risk register shows the rankings and the **best actions** for risk mitigation.

All Green and Yellow risk items have been reviewed with AOT and DII.

All High Risk (RED) items have been reviewed with AOT and DII. AOT has strived to resolve and mitigate as many of these identified risk as possible at this time. It is noted that AOT has worked diligently to address each of the High Risk areas for maximum risk reduction.

To date only six high-risk impact items remain on the risk mitigation risk register. Each of the following six (6) Risk items are still open and require action for closure and include:

1. Lack of enforcement by code for password policies.
2. Testing and User Acceptance Testing is performed in Delcan environment
3. Support and Maintenance is Task based and only for 14 days after delivery and acceptance.
4. Lack of current and up-to-date COOP and/or D/R Plan
5. Lack of compliance with respect to DII Security Standards policy
6. Lack of Independent Review for each TASK/SOW

ID	Item/Function Issue	Potential Risk Event	Severity of Event	S	Probability of Event	P	Current Controls (Detection)	C	PPN	Best Actions
Strategy and Funding										
S1	Non-alignment of MATS (legacy project) with 6 points for 2013 in 5 year plan for IT from DII	Not optimal or collaborative strategy		3		10		1	30	Meeting of parties and reconcile
S2	Currently, the MATS application is sole-sourced relying on DELCAN only	Custom developed solutions present a risk due to lack of industry standards and proprietary nature of solution		5		6		5	150	Develop contingency plan and examine COTS software
S3	MATS is developed using discrete 'Tasks' with limited consideration to an overall Roadmap. The last update was 2009	Lack of 'big picture' and shifts in technology and trends		5		10		3	150	Update 2009 Roadmap with concerned parties
S4	There does not appear to be a local documented SDLC for VT including development and user acceptance testing with respect to configuration and customization, support, maint.	Bugs, problems and failures due to adequate testing and acceptance		4		8		3	96	Document and implement testing, acceptance, roll-out and support plan
S5	Vtrans uses MATS for Time and Billing. The rest of VT will be using Vision			3		10		2	60	This issue needs to be reconciled. According to VTrans, there is a Fed. Reporting requirement that Vision is incapable of supporting
S6	Many users will use Citrix to access MATS in VT in the event of an emergency or security event	Citrix is supported by DII. If Citrix goes down, MATS will be unusable		10		6		8	480	Evaluate Citrix Risk and contingency plans. MATS/Vtrans need s to conduct a Risk Assessment That includes Citrix
S7	It was reported that DII could be taking over MATS support for servers, then application. "DII doesn't understand application"	Lack of support, and mistakes (at least 2 incidents to date). One resulting in MATS being down for 3 days		9		6		4	216	Develop strategy and plan with respect to Human Capital, IT and business alignment
Architecture and Technology										
A1	MATS uses a thick client interface. This arch. is platform specific, and results high total cost of ownership	Lack of flexibility during an event		7		8		2	112	Update Roadmap with concerned parties with respect to this issue
A2	There is little virtualization in use currently with MATS in VT	Lack of flexibility during an event		6		6		1	36	
A3	Lack of enforcement by code for password policies. This should include access logs for MATS	Security Breach		9		10		8	720	Add rules and functionality to code. Issue password guidelines to users. <u>OR</u> SSO using Active Directory
A4	STARS finance is being replaced by Vision in the next month	Changing systems is a risk		9		10		2	180	Document and test. Work with integration team. Delcan on-site
Human Capital Management										
H1	Within Vermont, MATS knowledge is concentrated among a few individuals. In some cases this is one or 2 individuals	Application knowledge goes with employee and is lost. This tribal undocumented knowledge represents a risk to the state.		9		4		2	72	Documentation
H2	Currently, there is no structured MATS training program	Inconsistent usage and deployment		2		3		1	6	Training If the business case supports it.
H3	The COOP plan has not been tested	MATS is unusable during an emergency 'event'		8		6		5	240	Test the COOP/DR Plan based on risks of the Risk Assessment
H4	Currently, DII is not equipped to support the 7x24x365 requirements of MATS	MATS or MATS users will be down		6		6		2	72	Develop plan and staffing. Create SLA
Tools & Process										
T1	There is little to no process documentation wrt MATS processes	Inability to analyze risk and vulnerabilities. Potential exposure.		6		3		2	36	Create the documentation per ANSI, IEEE or ISO
T2	Client/server approach is not best practice, platform specific, and high total cost of ownership	Unforeseen user issues. Upgrades and patches create issues on workstations. Vulnerabilities with respect to malware on client workstations. Platform specific.		6		5		3	90	Evaluate and update Roadmap with consideration to web and mobile technologies
T3	There is no on-line 'Help'	Loss in productivity		2		2		1	4	Address if the business case supports it.
T4	MATS issue reporting and release management is migrating to a new system	Change of systems is a risk		6		10		4	240	Test, train and roll-out
T5	The pre-configured reports are not flexible enough for end users.	Inability to report. Incorrect data		5		3		2	30	Address if the business case supports it.
T6	Testing and User Acceptance Testing is performed in Delcan environment	Local bugs, issues, and incidents		8		8		8	512	Stand up or re-allocate local VT environment
T7	Support and Maintenance is Task based and only for 14 days after delivery and acceptance.	There is no warranty or ongoing support and maintenance for the software		8		6		8	384	Address if the business case supports it.
T8	Existing documentation does not follow any accepted standards (ISO)	Incomplete or inaccurate documentation		2		2		1	4	Address if the business case supports it.
Data Management										
D1	With respect to Vision ERP, the data exchange file format is in flux and not defined. This issue is not unique to MATS and is indicative of a bigger issue and lack of a Master Data Model within the SoV	Payroll will not be met		9		8		8	576	Mitigation appears to be adequate Test and deliver to Vision desired format before deadline. Per Task 14, Delcan will be onsite
Governance, Risk, and Compliance										
G1	Non-Compliance with Information Resource Management Advisory Council Five-Year Plan for Information Technology	Contract and expenditure not approved		6		6		3	108	Create 5 year Plan per guidelines
G2	Non-Compliance with Information Resource Management Advisory Council Cost Benefit Analysis	Contract and expenditure not approved		6		6		3	108	Create Cost / Benefit Plan per guidelines
G3	Lack of current and up-to-date COOP and/or D/R Plan	MATS is unusable during an emergency 'event'		9		8		7	504	Revise plan
G4	Lack of 5 year Maintenance and support plan	Lack of 'big picture' and shifts in technology and trends Inability to support PPM		6		8		2	96	Create plan
G5	Currently, there is a lack of Key Performance Indicators and measurement criteria with respect to MATS and MATS OPS.	Required according to policy Loss of end user and constituent support Inability to measure tasks success (or not)		6		8		1	48	Implement measurements and Key Performance Indicators (kpi's)
G6	Non-compliance with source code requirements with respect to the State of Vermont (possession)	Legal action. Loss if IP and ability to support MATS		7		6		1	42	Download code from Delcan
G7	Lack of compliance with respect to DII Security Standards policy	Security Breach		7		8		8	448	Implement policies and procedures with Vendor
G8	Information Security - Pentest and Vulnerability Scan being performed by AOT and Delcan.	Security Breach of system		9		6		4	216	The scan and pentest need to be performed by a third party
G9	Lack of Independent Review for each TASK/SOW	Value and Best practice. Current process appears to circumvent intent of IR.		6		10		6	360	Program Project and Portfolio Management representation from DII

Remaining Risk Discussion and Explanation

With respect to the specific issues, or risk indications, they can for the most part be categorized into the follow:

Issue 1	Compliance with existing Vermont Information Technology policies
Assessment	The State has published policies and statutes in place. In many/most case, MATS, pre-dates these policies. Nonetheless the current state of MATS is non-compliant with the existing policies.
Implication	Non-compliance could result in a security breach, lack of funding and support...
Recommendation /Remediation	VTrans to secure a waiver (grandfathered-in) or create a plan for compliance

Issue 2	Compliance with Procurement and acquisition Policy
Assessment	<p>The State has published Policies in place with respect to IT purchases that exceed a threshold amount. Specific policies are:</p> <ul style="list-style-type: none"> • Cost Benefit Analysis; • Five Year Plan; • Independent Review; • Source Code policy. <p>In many/most case, MATS, and MATS procurement pre-dates these policies, and as such is currently non-compliant with respect to these policies. Other indications are the Roadmap for MATS was last updated in 2009, non-existent metrics and key performance indicators, or measurements of any kind to measure MATS performance against specific goals and objectives of the system.</p>
Implication	Lack of funding, or non-approval.
Recommendation /Remediation	VTrans to secure a waiver (grandfathered-in) or create a plan for compliance

Issue 3	<i>Continuity of Operations (COOP) and Disaster Recovery</i>
Assessment	Nonexistent, tested COOP plan. There are currently some mitigating factors, but this represents a significant risk to the State. Also, what-if scenarios need to be considered. If there is an event; like virus and malware spreading to VTrans workstations, or a down (LAN) network users will be accessing MATS via Citrix.
Implication	Lack of access to MATS, loss of data, breach or compromise
Recommendation /Remediation	Current and tested COOP Plan addresses the formal Risk Assessment of MATS. To date, a Risk Assessment has not been submitted to the IR.

Issue 4	<i>Structured Processes and methodologies with documentation</i>
Assessment	In many most cases, MATS (in Vermont) used ad hoc, or informal processes with little or no evident documentation, or in many cases, existing documentation was not kept up-to-date.
Implication	Specific processes (Testing and User Acceptance for example) especially need to be documented and follow industry accepted best practices. Software issues, unreliable/unexpected data/results, bugs, could be the resultant. With respect to PPM at the SoV level, documentation will be required for application rationalization and standardization.
Recommendation/Remediation	Leverage existing documentation (standards and templates), best practices with the SoV for the Vision and Vantage projects. (We believe this documentation exists).

Issue 5		
MATS and Business Alignment with respect to VT IT Strategic Plan Principles for the period 2013-2018		
Assessment	Findings	DII Principles fundamental for 2013 work:
	Yes	1. Leverage IT successes in other states.
	No	2. Leverage shared services and cloud-based IT.
	No	3. Leverage modern IT delivery frameworks.
	No	4. Realign the workforce to adapt to new IT and scale economies.
	Yes	5. Couple IT with business process optimization.
	Partial	6. Optimize IT investments via well-aligned Enterprise Architecture, Project Management, and Project Portfolio Management methodologies.
Implication	System redundancy/overlap, silos of automation, lack of efficiencies and higher cost, needless and expensive data exchanges and interfaces.	
Recommendation/Remediation	MATS Roadmap review with interested parties (DII). This should include, virtualization/consolidation, workforce alignment.	

Issue 6	
MATS Information Security	
Assessment	MATS does not hold any regulated data or PII according to all the documentation presented. MATS does represent a security risk based in current non-compliances with Vermont policy and practices in place. Indications of this are, scans and Penetration tests (pentests) need to be performed by independent parties (they were not). Vermont Security Standards with respect to Application Development needs to be implemented or at a minimum evaluated. Password policies need to be enforced using Active Directory or software with respect to authentication including access logging.
Implication	Security breach of MATS and potentially MATS servers.
Recommendation /Remediation	Integrated with Active Directory (in the next task?). Work with Delcan to implement policies and controls. Pentest/Scans by DII or other.

Issue 7	(MATS) Program and Portfolio Management (PPM)
Assessment	MATS' Tasks/SOW, with the MATS Roadmap need to be considered in the context of the projects and portfolio for the entire State of Vermont. For example, VTrans employees will be using MATS for Time Entry whereas the rest of Vermont have recently been trained and will be using Vision (PeopleSoft). Additionally, there is a strategic project with respect to Citrix for \$500k and a workflow system that may overlap with MATS. The \$200K-\$300k MATS also sort of fall under the radar at the current time from a PPM perspective
Implication	Silos of automation, duplication, inefficiencies, errors, expensive integrations to share data.
Recommendation/ Remediation	Strategic planning and discussions. Possible implementation of PPM software at the State level?

Issue 8	(MATS) Contract and Support
Assessment	MATS is currently sole-sourced to Delcan. This represents a potential risk if the vendor defaults. There is also some risk and exposure with respect to Warranty, Maintenance. and Support. Maintenance. and support only seem to apply to the specific tasks for a period of 14 days. There is no traditional support contract, as this is custom software.
Implication	Lack of MATS support and future control, legal exposure, Issues, bugs, etc.
Recommendation/ Remediation	Contingency plan with respect to Delcan, maintenance and support agreement. Discussions with Delcan as MATS a commercial Off the Shelf Application.

Detailed Risk “Best Actions” For Remediation

During the risk mitigation and recommendation portion of this Independent Review, Coeur Group identified each of the risk/issues and documented them in Coeur Group’s “Risk Action Register”. These Risks are defined in 5 Risk Domain areas which include; Strategy & funding, architecture and technology, human capital management, tools and processes, data and governance and compliance risk.

In addition each **potential risk event** was documented and a **best action** for risk remediation was identified, discussed and entered into the Risk Action Register.

The following are the detailed **“best actions”** to mitigate the quantified risk in the six (6) categorical risk domains.

Strategy and Funding Risks

ID	Item/Function Issue	Potential Risk Event	PRN	Best Actions
Strategy and Funding				
S1	Non-alignment of MATS [legacy project] with 6 points for 2013 in 5 year plan for IT from DII	Not optimal or collaborative strategy	30	Meeting of parties and reconcile
S2	Currently, the MATS application is sole –sourced relying on DELCAN only	Custom developed solutions present a risk due to lack of industry standards and proprietary nature of solution	150	Develop contingency plan and examine COTS software
S3	MATS is developed using discrete 'Tasks' with limited consideration to an overall Roadmap. The last update was 2009	Lack of 'big picture' and shifts in technology and trends	150	Update 2009 Roadmap with concerned parties
S4	There does not appear to be a local documented SDLC for VT including development and user acceptance testing with respect to configuration and customization, support, maint.	Bugs, problems and failures due to adequate testing and acceptance	96	Document and implement testing, acceptance, roll-out and support plan
S5	Vtrans uses MATS for Time and Billing. The rest of VT will be using Vision		60	This issue needs to be reconciled. According to VTrans, there is a Fed. Reporting requirement that Vision is incapable of supporting
S6	Many users will use Citrix to access MATS in VT in the event of a emergency or security event	Citrix is supportewd by DII. If Citrix goes down, MATS will be unusable	36	Evaluate Citrix Risk and contingency plans. MATS/Vtrans need s to conduct a Risk Assessment That includes Citrix
S7	It was reported that DII could be taking over MATS support for servers, then application. "DII doesn't understand application"	Lack of support, and mistakes (at least 2 incidents to date). One resulting in MATS being down for 3 days	216	Develop strategy and plan with respect to Human Capital, IT and business alignment

Architecture and Technology Risks

ID	Item/Function Issue	Potential Risk Event	PRN	Best Actions
Architecture and Technology				
A1	MATS uses a thick client interface. This arch. is platform specific, and results high total cost of ownership	Lack of flexibility during an event	112	Update Roadmap with concerned parties with respect to this issue
A2	There is little virtualization in use currently with MATS in VT	Lack of flexibility during an event	36	
A3	Lack of enforcement by code for password policies. This should include access logs for MATS	Security Breach	720	Add rules and functionality to code. Issue password guidelines to users. OR SSO using Active Directory
A4	STARS finance is being replaced by Vision in the next month	Changing systems is a risk	180	Document and test. Work with integration team. Delcan on-site

Human Capital Management Risks

ID	Item/Function Issue	Potential Risk Event	PRN	Best Actions
Human Capital Management				
H1	Within Vermont, MATS knowledge is concentrated among a few individuals. In some case this is one or 2 individuals	Application knowledge goes with employee and is lost. This tribal undocumented knowledge represents a risk to the state.	72	Documentation
H2	Currently, there is no structured MATS training program	Inconsistent usage and deployment	6	Training if the business case supports it.
H3	The COOP plan has not been tested	MATS is unusable during an emergency 'event'	240	Test the COOP/DR Plan based on risks of the Risk Assessment
H4	Currently, DII is not equipped to support the 7x24x365 requirements of MATS	MATS or MATS users will be down	72	Develop plan and staffing. Create SLA

Tools and Processes Risks

ID	Item/Function Issue	Potential Risk Event	PRN	Best Actions
Tools & Process				
T1	There is little to no process documentation wrt MATS processes	Inability to analyze risk and vulnerabilities. Potential exposure.	36	Create the documentation per ANSI, IEEE or ISO
T2	Client/server approach is not best practice, platform specific, and high total cost of ownership	Unforeseen user issues. Upgrades and patches create issues on workstations. Vulnerabilities with respect to malware on client workstations. Platform specific.	90	Evaluate and update Roadmap with consideration to web and mobile technologies
T3	There is no on-line 'Help'	Loss in productivity	4	Address if the business case supports it.
T4	MATS issue reporting and release management is migrating to a new system	Change of systems is a risk	240	Test, train and roll-out
T5	The pre-configured reports are not flexible enough for end users.	Inability to report. Incorrect data	30	Address if the business case supports it.
T6	Testing and User Acceptance Testing is performed in Delcam environment	Local bugs, issues, and incidents	512	Stand up or re-allocate local VT environment
T7	Support and Maintenance is Task based and only for 14 days after delivery and acceptance.	There is no warranty or ongoing support and maintenance for the software	384	Address if the business case supports it.
T8	Existing documentation does not follow any accepted standards (ISO)	Incomplete or inaccurate documentation	4	Address if the business case supports it.

Data Management Risks

ID	Item/Function Issue	Potential Risk Event	PRN	Best Actions
Data Management				
D1	With respect to Vision ERP, the data exchange file format is in flux and not defined. This issue is not unique to MATS and is indicative of a bigger issue and lack of a Master Data Model within the SoV	Payroll will not be met	576	Mitigation appears to be adequate Test and deliver to Vision desired format before deadline. Per Task 14, Delcam will be onsite

Governance Risk, and Compliance Risks

ID	Item/Function Issue	Potential Risk Event	PRN	Best Actions
Governance, Risk, and Compliance				
G1	Non-Compliance with Information Resource Management Advisory Council Five-Year Plan for Information Technology	Contract and expenditure not approved	108	Create 5 year Plan per guidelines
G2	Non-Compliance with Information Resource Management Advisory Council Cost Benefit Analysis	Contract and expenditure not approved	108	Create Cost / Benefit Plan per guidelines
G3	Lack of current and up-to-date COOP and/or D/R Plan	MATS is unusable during an emergency 'event'	504	Revise plan
G4	Lack of 5 year Maintenance and support plan	Lack of 'big picture' and shifts in technology and trends Inability to support PPM	96	Create plan
G5	Currently, there is a lack of Key Performance Indicators and measurement criteria with respect to MATS and MATS OPS.	Required according to policy Loss of end user and constituent support Inability to measure tasks success (or not)	48	Implement measurements and Key Performance Indicators (kpi's)
G6	Non-compliance with source code requirements with respect to the State of Vermont (possession)	Legal action. Loss if IP and ability to support MATS	42	Download code from Delcan
G7	Lack of compliance with respect to DII Security Standards policy	Security Breach	448	Implement policies and procedures with Vendor
G8	Information Security - Pentest and Vulnerability Scan being performed by AOT and Delcan.	Security Breach of system	216	The scan and pentest need to be performed by a third party
G9	Lack of Independent Review for each TASK/SOW	Value and Best practice. Current process appears to circumvent intent of IR.	360	Program Project and Portfolio Management representation from DII

**Best Actions for Remediation for Interim Open Items
(as of 7/01/2013)**

Open Issue #1: Lack of current and up-to-date COOP and/or D/R Plan

Potential Risk Event: MATS is unusable during an emergency 'event'

PRN = 504

Action Recommended: Revise plan

1. *AOT Pre-Contract Action:* AOT has a COOP Plan that will be updated to include MATS. As part of this plan a Risk Assessment for MATS will be performed & included in the plan.
2. *AOT Pre-Contract Action:* AOT is working to define the DR and COOP. AOT DR infrastructure is in place. Next step is to test with MATS to see if infrastructure can support MATS or if additional hardware may be needed. Due to ERP implementation, MATS DR testing may not take place until July and the COOP finalized sometime in August/September timeframe. Failover procedures will be included.
3. *AOT Future Commitment/No Pre-Contract Action:* AOT will create & implement a plan for annual testing of the COOP & DR plan with regard to MATS. "

Current Disposition: Non-acceptable. At this time there was no Disaster Recovery Test submitted, the plan was incomplete and work in process. The Risk Assessment was incomplete and consisted of 2 items

Recommendation: This is Non-critical to steady state system operations. However since a lack of a formal COOP plan increases the overall risk of MATS operations, DII should proceed with contract and work with VTrans to develop a COOP plan and testing in-line with the State's policies regarding *Critical Systems*.

Issue #2: Lack of compliance with respect to DII Security Standards policy

Potential Risk Event: Security Breach

PRN = 448

Action Recommended: Implement policies and procedures with Vendor

1. *AOT Pre-Contract Action:* Complete a Business Case & Cost Model specifically for the new Delcan contract and the enhancements being pursued as part of this contract.
2. Comply with the Password Policy.

Current Disposition: Non-Acceptable. Limited and incomplete submissions with respect to Business case, Cost Model, and MATS Roadmap as required by statute.

Recommendation: Non-critical to system Operation. AOT should work with DII and DII/CIO to produce a Security Plan and documentation in line with State policies and expectations.

Issue #3: Lack of Independent Review for each TASK/SOW can provide potential for cost over runs.

Potential Risk Event: Current process appears to circumvent intent of IR.

PRN = 360

Action Recommended: Program Project and Portfolio Management representation from DII

1. AOT Pre-Contract Action: Complete a 5 Year Road Map for MATS

Current Disposition: Non-acceptable as a normal standard for managing implementation plans and performance. At this time as there was no roadmap to reconcile with the entire expenditure

Recommendation: Non-Critical to business operations of MATS. AOT should work with DII/CIO to reconcile the implementation planning process for AOT improvement Statements of Work.

Summary

MATS is currently in use, successful, and widely deployed in Vermont, New Hampshire, and Maine. The core functionality for time entry, work order management, asset management, planning and budgeting, is also performed in many other departments across the State of Vermont. There may be unique and valid business reasons as to why VTrans (and others) need a specially developed and unique application.

Key Cost Impact Issue:

Based on the initial timeframe for startup of this project in 1997, there were not many Commercial Off the Shelf (COTS) systems to perform these Asset Management “Business Requirements” needed by Vermont and the Tri-state program. A key issue for the State of Vermont today is to review future requirements of the AOT-MATS system and determine if COTS modules would be appropriate or even available to reduce **Application Development** costs from the current vendor Delcan. This may be an opportunity for cost savings.

The MATS application to date has by and large been driven by specific requirements that are submitted as Tasks. These tend to be features and functions that the constituents want and need and add value to them. Unfortunately, this organic and grass roots development does not place equal

weight on non-ROI items – at the user level –like security, application architecture, system and user administration. The result is a system that is client/server (thick client) based, some web enablement/support, highly custom, platform specific, and has minimal (application) security built in and I suspect has a high Total Cost of Ownership (TCO) when all things are considered.

With respect to this IR of April – June of 2013, the review can only be conducted with respect to the Tasks (SoW) submitted and the costs provided for that corresponding SoW.

The IR process for the entire authorized expenditure of four million dollars (\$4M) cannot be addressed at this time. Some potential risk items are still preventient due to the limited responses for certain items at the time of this review and remain undeterminable for purposes of this Independent Review.

Final Risk Disposition (as of 8/01/2013)

The following Risk Register provides the final disposition of all identified risks. The risks resolutions have been agreed to between DII and AOT and a plan from AOT to DII for final resolution of each. All are currently Work In Progress (WIP) for resolution and these include; A3, H3, T6, T7, G3 and G9.

Final IR Session 7/29/2013

Attendees:

AOT: Robert White, And Morse, Tom Hurd and Betsy Ross-Mobbs
Coeur Group by phone: Mark Peterson, Bob Carroll and Dan McClane
DII: Richard Boes and Martha Haley

The group walked through Appendix F (IR Disposition of Risk Considering Final Submissions) of the IR report. Here are the results of that discussion:

A3: The password enhancements are currently in testing. Some issues were identified and were reported to Delcan. Delcan is fixing the issues. AOT expects to implement the password functionality with the next release in about 2 weeks.

T6 & T7: These will be addressed with the same solution which is to add language to the contract to require Delcan to fix problems/issues with the software when they are identified, rather than the 14 day warranty that is stated in the current contract. A change to this language would be consist with what Delcan has been doing, just not what they are contractually obligated to do.

D1: This issue was previously closed.

G3: The Capitol Press Building at the airport is AOT's current, but temporary, back-up site. The plan is to prioritize MATS early in the I-TOP server transition and potentially leverage DII's new secondary data center at Tech Vault. Tom Hurd will discuss this further with Michael Morey. In addition, AOT committed to continuously improving the quality and completeness of both their COOP and DR plans.

G7: Issues were specific to security and this item is covered by A3.

G9: Richard requested that AOT provide an updated Business Case and Cost Model. He needs to have a clear understanding of all costs before approving a new Delcan contract.

Summary of Final Results:

- Approval of the IR report & Completion of the IR Engagement:** Coeur Group provided clarification on item G7 and this is covered by item A3.
- MATS Contract Approval:** The testing/warranty issue (T6 & T7) needs to be addressed in the new contract. In addition, a CIO approved Business Case and Cost Model are required to obtain contract approval.

The IR Risk Register below shows the Final Disposition of all identified Risks for this Independent review.

ID	Item/Function Issue	Potential Risk Event	Severity of Event	S	Probability of Event	P	Current Controls (Detection)	C	PRN	Final IR Disposition
Strategy and Funding										Open - WIP-Closed
S1	Non-alignment of MATS [legacy project] with 6 points for 2013 in 5 year plan for IT from DII	Not optimal or collaborative strategy		3		10		1	30	c
S2	Currently, the MATS application is sole-sourced relying on DELCAN only	Custom developed solutions present a risk due to lack of industry standards and proprietary nature of solution		5		6		5	150	c
S3	MATS is developed using discrete 'Tasks' with limited consideration to an overall Roadmap. The last update was 2009	Lack of 'big picture' and shifts in technology and trends		5		10		3	150	c
S4	There does not appear to be a local documented SDLC for VT including development and user acceptance testing with respect to configuration and customization, support, maint.	Bugs, problems and failures due to adequate testing and acceptance		4		8		3	96	c
S5	Vtrans uses MATS for Time and Billing. The rest of VT will be using Vision			3		10		2	60	c
S6	Many users will use Citrix to access MATS in VT in the event of a emergency or security event	Citrix is supportewd by DII. If Citrix goes down, MATS will be unusable		4		3		3	36	c
S7	It was reported that DII could be taking over MATS support for servers, then application. "DII doesn't understand application"	Lack of support, and mistakes (at least 2 incidents to date). One resulting in MATS being down for 3 days		9		6		4	216	c
Architecture and Technology										
A1	MATS uses a thick client interface. This arch. is platform specific, and results high total cost of ownership	Lack of flexibility during an event		7		8		2	112	c
A2	There is little virtualization in use currently with MATS in VT	Lack of flexibility during an event		6		6		1	36	c
A3	Lack of enforcement by code for password policies. This should include access logs for MATS	Security Breach		9		10		8	720	w
A4	STARS finance is being replaced by Vision in the next month	Changing systems is a risk		9		10		2	180	c
Human Capital Management										
H1	Within Vermont, MATS knowledge is concentrated among a few individuals. In some case this is one or 2 individuals	Application knowledge goes with employee and is lost. This tribal undocumented knowledge represents a risk to the state.		9		4		2	72	c
H2	Currently, there is no structured MATS training program	Inconsistent usage and deployment		2		3		1	6	c
H3	The COOP plan has not been tested	MATS is unusable during an emergency 'event'		8		6		5	240	w
H4	Currently, DII is not equipped to support the 7x24x365 requirements of MATS	MATS or MATS users will be down		6		6		2	72	c
Tools & Process										
T1	There is little to no process documentation wrt MATS processes	Inability to analyze risk and vulnerabilities. Potential exposure.		6		3		2	36	c
T2	Client/server approach is not best practice, platform specific, and high total cost of ownership	Unforseen user issues. Upgrades and patches create issues on workstations. Vulnerabilities with respect to malware on client workstations. Platform specific.		6		5		3	90	c
T3	There is no on-line 'Help'	Loss in productivity		2		2		1	4	c
T4	MATS issue reporting and release management is migrating to a new system	Change of systems is a risk		6		10		4	240	c
T5	The pre-configured reports are not flexible enough for end users.	Inability to report. Incorrect data		5		3		2	30	c
T6	Testing and User Acceptance Testing is performed in Delcan environment	Local bugs, issues, and incidents		8		8		8	512	w
T7	Support and Maintenance is Task based and only for 14 days after delivery and acceptance.	There is no warranty or ongoing support and maintenance for the software		8		6		8	384	w
T8	Existing documentation does not follow any accepted standards (ISO)	Incomplete or inaccurate documentation		2		2		1	4	c

Data Management										
D1	With respect to Vision ERP, the data exchange file format is in flux and not defined. This issue is not unique to MATS and is indicative of a bigger issue and lack of a Master Data Model within the SoV	Payroll will not be met		9		8		8	576	c
Governance, Risk, and Compliance										
G1	Non-Compliance with Information Resource Management Advisory Council Five-Year Plan for Information Technology	Contract and expenditure not approved		6		6		3	108	c
G2	Non-Compliance with Information Resource Management Advisory Council Cost Benefit Analysis	Contract and expenditure not approved		6		6		3	108	c
G3	Lack of current and up-to-date COOP and/or D/R Plan	MATS is unusable during an emergency event		9		8		7	504	w
G4	Lack of 5 year Maintenance and support plan	Lack of 'big picture' and shifts in technology and trends Inability to support PPM		6		8		2	96	c
G5	Currently, there is a lack of Key Performance Indicators and measurement criteria with respect to MATS and MATS OPS.	Required according to policy Loss of end user and constituent support Inability to measure tasks success (or not)		6		8		1	48	c
G6	Non-compliance with source code requirements with respect to the State of Vermont (possession)	Legal action. Loss if IP and ability to support MATS		7		6		1	42	c
G7	Lack of compliance with respect to DII Security Standards policy	Security Breach		7		8		8	448	c
G8	Information Security - Pentest and Vulnerability Scan being performed by AOT and Delcan.	Security Breach of system		9		6		4	216	c
G9	Lack of Independent Review for each TASK/SOW	Value and Best practice. Current process appears to circumvent intent of IR.		6		10		6	360	w

Appendix A – Project Cost Details

Delcan has provided the following list as Current Contract Period 2013 -> 2017

Major Tasks and Deliverables:

ID	Cost	Completion	Deliverables Description
1	\$245,000 (VT)	7/15/2013	Task 14 VT Payroll Implementation. The State of Vermont Agency of Transportation (VVTRANS) is requesting services to coordinate with the changes required by the ERP Implementation
2	\$225,000 (ME)	6/21/2013	Task 15 General Enhancements and additional Admin. Screen. The State of Maine would like to undertake enhancements to Managing Assets on Transportation Systems (MATS) system. This would involve additional administration screens, stop select list screens from refreshing on receiving the focus, Modifications that improve the State of Maine (MeDOT's) approval reports and process, modifications the reflect the changes to how MATS is used for work planning, and improvements to the procedure of inactivating assets.
	\$470,000	Total allocated for Delcan	
	\$4,000,000	Budget/ Contract Total	
	\$3,530,000	NOT allocated as of 4/2013	

Prior Contract Period 2009 -> 2013 Major Tasks and Deliverables

ID	Cost	Year	Vermont Only Amt.	
1	\$1,320,000	2009	\$485,000	
2	\$975,000	2010	\$580,000	
3	\$350,000	2011	\$100,000	
4	0	2012		
	\$2,645,000	Total Spend with Delcan		\$1,165,000 44%*
	\$4,000,000	Budget/ Contract Total		
	\$1,355,000	Undetermined spend for this IR		

* It should be noted that for the prior contract period, Vermont funded 44% of the total cost. A chart with the historical data is available in the appendix.

Appendix B – Original Risks Summary

Risk Details by Domain All Scores

For the purposes of aggregation and analysis the risk indications were categorized:

1. Strategy and Funding
2. Architecture and Technology
3. Human Capital Management
4. Tools and Processes
5. Data Management
6. Governance, Risk, and Compliance (Std. IT nomenclature)

The Following Charts show the detail of the Potential Risk Number analysis and identification of the Potential Risk Event if not mitigated.

Strategy and Funding

ID	Item/Function Issue	Potential Risk Event	Severity of Event	S	Probability of Event	P	Current Controls (Detection)	C	PRN
Strategy and Funding									
s1	Non-alignment of MATS [legacy project] with 6 points for 2013 in 5 year plan for IT from DII	Not optimal or collaborative strategy		3		10		1	30
s2	Currently, the MATS application is sole-sourced relying on DELCAN only	Custom developed solutions present a risk due to lack of industry standards and proprietary nature of solution		5		6		5	150
s3	MATS is developed using discrete 'Tasks' with limited consideration to an overall Roadmap. The last update was 2009	Lack of 'big picture' and shifts in technology and trends		5		10		3	150
s4	There does not appear to be a local documented SDLC for VT including development and user acceptance testing with respect to configuration and customization, support, maint.	Bugs, problems and failures due to adequate testing and acceptance		4		8		3	96
s5	Vtrans uses MATS for Time and Billing. The rest of VT will be using Vision			3		10		2	60
s6	Many users will use Citrix to access MATS in VT in the event of a emergency or security event	Citrix is supportewd by DII. If Citrix goes down, MATS will be unusable		4		3		3	36
s7	It was reported that DII could be taking over MATS support for servers, then application. "DII doesn't understand application"	Lack of support, and mistakes (at least 2 incidents to date). One resulting in MATS being down for 3 days		9		6		4	216

Architecture and Technology

ID	Item/Function Issue	Potential Risk Event	Severity of Event	S	Probability of Event	P	Current Controls (Detection)	C	PRN
Architecture and Technology									
A1	MATS uses a thick client interface. This arch. is platform specific, and results high total cost of ownership	Lack of flexibility during an event		7		8		2	112
A2	There is little virtualization in use currently with MATS in VT	Lack of flexibility during an event		6		6		1	36
A3	Lack of enforcement by code for password policies. This should include access logs for MATS	Security Breach		9		10		8	720
A4	STARS finance is being replaced by Vision in the next month	Changing systems is a risk		9		10		2	180

Human Capital Management

ID	Item/Function Issue	Potential Risk Event	Severity of Event	S	Probability of Event	P	Current Controls (Detection)	C	PRN
Human Capital Management									
H1	Within Vermont, MATS knowledge is concentrated among a few individuals. In some case this is one or 2 individuals	Application knowledge goes with employee and is lost. This tribal undocumented knowledge represents a risk to the state.		9		4		2	72
H2	Currently, there is no structured MATS training program	Inconsistent usage and deployment		2		3		1	6
H3	The COOP plan has not been tested	MATS is unusable during an emergency 'event'		8		6		5	240
H4	Currently, DII is not equipped to support the 7x24x365 requirements of MATS	MATS or MATS users will be down		6		6		2	72

Tools and Processes

ID	Item/Function Issue	Potential Risk Event	Severity of Event	S	Probability of Event	P	Current Controls (Detection)	C	PRN
Tools & Process									
T1	There is little to no process documentation wrt MATS processes	Inability to analyze risk and vulnerabilities. Potential exposure.		6		3		2	36
T2	Client/server approach is not best practice, platform specific, and high total cost of ownership	Unforeseen user issues. Upgrades and patches create issues on workstations. Vulnerabilities with respect to malware on client workstations. Platform specific.		6		5		3	90
T3	There is no on-line 'Help'	Loss in productivity		2		2		1	4
T4	MATS issue reporting and release management is migrating to a new system	Change of systems is a risk		6		10		4	240
T5	The pre-configured reports are not flexible enough for end users.	Inability to report. Incorrect data		5		3		2	30
T6	Testing and User Acceptance Testing is performed in Delcan environment	Local bugs, issues, and incidents		8		8		8	512
T7	Support and Maintenance is Task based and only for 14 days after delivery and acceptance.	There is no warranty or ongoing support and maintenace for the software		8		6		8	384
T8	Existing documentation does not follow any accepted standards (ISO)	Incomplete or inaccurate documentation		2		2		1	4

Data Management

ID	Item/Function Issue	Potential Risk Event	Severity of Event	S	Probability of Event	P	Current Controls (Detection)	C	PRN
Data Management									
D1	With respect to Vision ERP, the data exchange file format is in flux and not defined. This issue is not unique to MATS and is indicative of a bigger issue and lack of a Master Data Model within the SoV	Payroll will not be met		9		8		8	576

Governance Risk, and Compliance

ID	Item/Function Issue	Potential Risk Event	Severity of Event	S	Probability of Event	P	Current Controls (Detection)	C	PRN
Governance, Risk, and Compliance									
G1	Non-Compliance with Information Resource Management Advisory Council Five-Year Plan for Information Technology	Contract and expenditure not approved		6		6		3	108
G2	Non-Compliance with Information Resource Management Advisory Council Cost Benefit Analysis	Contract and expenditure not approved		6		6		3	108
G3	Lack of current and up-to-date COOP and/or D/R Plan	MATS is unusable during an emergency 'event'		9		8		7	504
G4	Lack of 5 year Maintenance and support plan	Lack of 'big picture' and shifts in technology and trends Inability to support PPM		6		8		2	96
G5	Currently, there is a lack of Key Performance Indicators and measurement criteria with respect to MATS and MATS OPS.	Required according to policy Loss of end user and constituent support Inability to measure tasks success (or not)		6		8		1	48
G6	Non-compliance with source code requirements with respect to the State of Vermont (possession)	Legal action. Loss if IP and ability to support MATS		7		6		1	42
G7	Lack of compliance with respect to DII Security Standards policy	Security Breach		7		8		8	448
G8	Information Security - Pentest and Vulnerability Scan being performed by AOT and Delcan.	Security Breach of system		9		6		4	216
G9	Lack of Inedependant Review for each TASK/SOW	Value and Best practice. Current process appears to circumvent intent of IR.		6		10		6	360

Appendix C – Delcan Statement of Work (Tasks)

STATEMENT OF WORK (14)

For

Payroll Implementation

General

The State of Vermont Agency of Transportation (VAOT) is requesting services to coordinate with the changes required by the ERP Implementation.

The task is to be issued and administered by the Vermont Agency of Transportation (VAOT) in accordance with the provisions of the Tri-State Program Contract (#XXXXXX), with Vermont AOT providing technical direction for the work, as well as review and acceptance of work results.

Key Activities and Objectives

The key activities and objectives to be addressed by this effort will provide:

- ❖ Daily Employee Load
 - Create interface based on existing file format
- ❖ Bi-weekly Employee Load
 - Convert procedures to full Client Procedure format
- ❖ Payroll Submittal from ERP/STARS feedback loop
 - Create interface to store the ‘pay data’
 - Create timesheet report for signature
 - Ensure higher assignment pay is properly reported
- ❖ Payroll Export
 - Rename header file so that it is sequential
 - Full run-through on client site to enhance end-MATS-user integration with ERP (work within existing ERP limits)
- ❖ Employer/Employee History/Work Report Labor
 - Provide additional enhancements to address changes in ERP such as employee group/work schedule, Work Report Labor constraint to prevent Employer/Employee History contamination, Employee History ripple effects from late notice Labor Class Changes, etc.
- ❖ Edit checks
 - Provide an edit check report to account for up to 10 basic rules like preventing temps from using holiday pay, employees accounting for more/less than nominal hours, etc.
- ❖ Auto-install
 - Roll up to version 2

- ❖ Database Procedure refinements
 - Confirm all MATS procedures all rolled over to U2 standard
 - Remove all obsolete procedures
- ❖ DWR – Ripple-effect from DWR upgrade
 - Refine reports based (supervisor labor report double click still sends to old DWR)
 - Refine auto-date limits
- ❖ Provide access to the Delcan Requirements
- ❖ Configuration Objects
 - Identify what type of setting should be used for each object and adjust the existing data as necessary.
- ❖ Provide support up through July 15, 2013
 - Provide up to 20 additional refinements
 - Provide a Full build with all functionality identified by May 15
 - Provide up to one maintenance patch
 - Provide CTA test environment

The final product will be a software release that is production ready.

Desired Results

1. Successful development of 7.5.6 (or higher) that accounts for all identified items.

Other Requirements

The Tri-State Partnership will have rights to the documentation, work results, and information associated with this task.

STATEMENT OF WORK (15)

For

General Enhancements and additional Admin Screen**General**

The State of Maine would like to undertake enhancements to Managing Assets on Transportation Systems (MATS) system. This would involve additional administration screens, stop select list screens from refreshing on receiving the focus, Modifications that improve MeDOT's approval reports and process, modifications that reflect the changes to how MATS is used for work planning, and improvements to the procedure of inactivating assets.

The Tri-Partnership States decided that Maine will sponsor this enhancement. The task is to be issued and administered by the Vermont Agency of Transportation (VAOT) in accordance with the provisions of the Tri-State Partnership for Maintenance Management Contract (# PS0007) with Maine DOT providing technical direction for the work, as well as review and acceptance of work results.

Overview of General Enhancements and Admin Screens Effort

Because of the fluid nature of MeDOT's business process, minor changes are required to several screens. There are still administrative tasks still accomplished by Office of Information Technology that best done by business personnel using administrative screens.

Admin Screens

- Copy Contractor Costs (Like Copy Labor Rates)
- Contractor Cost Admin (Like Labor Rates)
- Activity Parent Tree View Screen (Scopes)
- Fiscal Year Tree View Admin Screen
 - o Fringe Factor Tab
 - o Labor Class Rate
 - o Equipment Class Rate
 - o Material Class Rate
 - o Contractor Cost
- Unit Pick List Management
 - o Tree View

List Screens

Please do not refresh the list when the screen receives the focus

- EA List Screen
- DWR List Screen
- Work Request List Screen
- ???

DWR List Screen

- Remove Special Event field
- Add Strom Event field

Sort List by Town Name

Daily Work Report

DWR List Screen

- Ability to save group ordering (Like Approvals) Detail
- Please add configuration item to set default DWR date
- Validation of Accomplishment (Based on Activity Standard)
- Validation of Equipment Hours (Based on 24 Hr. Day)
- Lock Stockpile Tab (Same as Locking the Core)
- Please add open asset button on asset detail on asset tab
 - o Use same open asset by number function as on menu
- Please add an manage stockpile button on stockpile tab
 - o Use Material Management User Entry Screen for Stockpile
- Please allow sort order for hour code on Employee tab
 - o Modify Hour Code admin screen to add sort order field

DWR Approval Screens

- Please remove hyperlink for the DWR.

Status History List Screen Read Only

- Filter by Status
- Type
- Filter by DWR Number

Planning and Budgeting

- Return to using Unit Work Responsibility for calculating inventory instead of unit hierarchy.
- Allow application to copy from Unit 0 - VIEW STATEWIDE DATA to Unit 0 - VIEW STATEWIDE DATA
- When creating the Fiscal Years, restore ability to load inventories, contractor costs rates, and activity/feature cross-reference

- Create admin screens for copying fringe factor, inventories, contractor costs rates, unit work responsibility, and activity/feature; pattern after the copy labor, equipment, and materials screens.
- Create admin screen for editing contractor costs rates.

Budget Request

- Add Summary of Accomplishments from Activity Plan Tab

Work Request

List

- Add Scope as a filter item (Below Date Filter)
- Add Expenditure Account
- Remove Compliance Filter

Detail – Core

- Add General Location (Description)
- Add General Route (Description)

Hierarchy – Based on User Level

- Corridor Scopes
- Types

Asset

Tabs

- When end dating the core records please end date all tab records.
- When removing end date please remove end dates all tab records.
- Roll up tab header like the header on core.
- Multiple row tabs so as not to need to “arrow” to locate other tabs
- Order asset tabs in all cases as follows –core, map, map (configurable?)

Location Control

- Validation of GIS Location (Using interface with GIS System)
- **Currently the Sync button will return a single mile point derived from the X/Y coordinate from the GIS-Decimal tab and populate the Begin MP and End MP fields when the primary location value is set at GIS-Decimal. When the Primary location value is set to RLM it will return a single X/Y coordinate derived from the route and Begin MP and populate the X_Long and Y_lat fields on the GIS-Decimal tab.**
- **What we would like the Sync button to do is have the ability to make a second call if it encounters a second set of Lat Longs, returned in order of the Sequence value, and return that as the End MP as well as return a second lat long and place them in the second line on the GIS-Decimal tab if it**

encounters an End MP. Potentially it would need to then populate the sequence values as well.

Picture Loader Enhancements

- Add Tagging Ability (Geo-Tagging)
- Have multi select ability when adding pictures

Security Administration

- Ability to manage each user type differently
- Add and manage different user types
- Use group security set at the admin level to tell which user type the logged in user can manage

Web Tab Administration

- The ability to apply security to tabs on the tab browser
- Add new field as a Description

Web Tab Browser

- Make tabs visible based on permissions set on be web tab admin
- Show Description With URL
 - 1) so people know what they are selecting

Expenditure Account

- Separate funding for labor, equipment, and materials
- Update procedures for Transactions to use new functionality
- On entry edit for default WIN's

Relationship to Other Systems/Capabilities

The dimensional data mart effort will leverage or work in conjunction with systems of authority when applicable that may include the following:

- FINISS - MDOT's Financial Enterprise System does Receivables, Transfers, Journals and Cash Receipts. In addition, it interacts with the Federal IT systems, FMIS (Fiscal Management Information System) and RASPS (Rapid Approval and state Payments System
- FREE2000 – MDOT's system for Exception Employee Time and Attendance, Employee Profiles, Leave Balances, Travel Requests and Reimbursements, and Invoice Payments.

Other Requirements

The Tri-State Partnership will have rights to all documentation, work results, and information associated with this task.

This Page Intentionally Left Blank

Appendix D – Open High Risk Item Details

ID	Item/Function Issue	Potential Risk Event	PRN	Coeur Recommendation	AOT Risk Strategy	AOT Artifact/ Evidence to be Reviewed at 6/4 Meeting?	Second Artifact (if applicable)	Third Artifact (if applicable)
Architecture & Technology								
A3	Lack of enforcement by code for password policies. This should include access logs for MATS	Security Breach	720	Add rules and functionality to code. Issue password guidelines to users. OR SSO using Active Directory	AOT Pre-Contract Action: AOT will implement the MATS Release that includes Password enforcement. AOT will provide the release related documentation for this enhancement as evidence that it meets DII's Password Policy.	https://inside.vermont.gov/projects/AOT%20MATS%20IR/Shared%20Documents/IR%20Artifacts%20from%20AOT/IR%20Meeting%20Artifacts/FW%20MATS%20Passwords.msg		
Tool & Process								
T6	Testing and User Acceptance Testing is performed in Delcan environment	Local bugs, issues, and incidents	512	Stand up or re-allocate local VT environment	<ol style="list-style-type: none"> AOT Future Commitment/ No Pre-Contract Action Needed: AOT performs their own testing on all enhancements. Documentation will now be kept by AOT on test scenarios and results for each new MATS release. AOT Pre-Contract Action: Contract currently only allows 14 days to identify issues with a new release. This does not allow adequate time for testing. AOT will negotiate an extension for this provision to 30 days. 	https://inside.vermont.gov/projects/AOT%20MATS%20IR/Shared%20Documents/IR%20Artifacts%20from%20AOT/IR%20Meeting%20Artifacts/UPGRADE TEST MATS New module release.docx		

Tool & Process							
T7	Support and Maintenance is Task based and only for 14 days after delivery and acceptance.	There is no warranty or ongoing support and maintenance for the software	384	Address if the business case supports it.	<p>1. See #2 in T6.</p> <p>2. No Action Needed: The State owns the code & has developed expertise in-house to support it, so AOT doesn't need to spend State money on a Maintenance Agreement with Delcan. If/When needed, AOT can contract with Delcan for specific maintenance tasks.</p>	No	

Governance, Risk & Compliance							
G3	Lack of current and up-to-date COOP and/or D/R Plan	MATS is unusable during an emergency 'event'	504	Revise plan	<p>1. AOT Pre-Contract Action: AOT has a COOP Plan that will be updated to include MATS. As part of this plan a Risk Assessment for MATS will be performed & included in the plan.</p> <p>2. AOT Pre-Contract Action: AOT is working to define the DR and COOP. AOT DR infrastructure is in place. Next step is to test with MATS to see if infrastructure can support MATS or if additional hardware may be needed. Due to ERP implementation, MATS DR testing may not take place until July and the COOP finalized sometime in August/September timeframe. Failover procedures will be included.</p> <p>3. AOT Future Commitment/No Pre-Contract Action: AOT will create & implement a plan for annual testing of the COOP & DR plan with regard to MATS.</p>	<p>https://inside.vermont.gov/projects/AOT%20MATS%20IR/Shared%20Documents/IR%20Artifacts%20from%20AOT/IR%20Meeting%20Artifacts/OPS_MATS%20Security_DR_Plan-06102013.docx</p>	<p>https://inside.vermont.gov/projects/AOT%20MATS%20IR/Shared%20Documents/IR%20Artifacts%20from%20AOT/IR%20Meeting%20Artifacts/FW%20AOT%20COOP%20-%20Final.msg</p>

Appendix E – Initial Risk Strategy and Submissions

The following tables reflect the outcomes and actions following the DRAFT review, and additional and revised submissions from VTrans.

ID	Item/Function Issue	Potential Risk Event	PRN	Coeur Recommendation	AOT Risk Strategy	AOT Artifact/ Evidence to be Reviewed at 6/4 Meeting?	Second Artifact (if applicable)	Third Artifact (if applicable)
Architecture & Technology								
A3	Lack of enforcement by code for password policies. This should include access logs for MATS	Security Breach	720	Add rules and functionality to code. Issue password guidelines to users. OR SSO using Active Directory	AOT Pre-Contract Action: AOT will implement the MATS Release that includes Password enforcement. AOT will provide the release related documentation for this enhancement as evidence that it meets DII's Password Policy.	https://inside.vermont.gov/projects/AOT%20MATS%20IR/Shared%20Documents/IR%20Artifacts%20from%20AOT/IR%20Meeting%20Artifacts/FW%20MATS%20Passwords.msg		
Tool & Process								
T6	Testing and User Acceptance Testing is performed in Delcan environment	Local bugs, issues, and incidents	512	Stand up or re-allocate local VT environment	<p>1. AOT Future Commitment/ No Pre-Contract Action Needed: AOT performs their own testing on all enhancements. Documentation will now be kept by AOT on test scenarios and results for each new MATS release.</p> <p>2. AOT Pre-Contract Action: Contract currently only allows 14 days to identify issues with a new release. This does not allow adequate time for testing. AOT will negotiate an extension for this provision to 30 days.</p>	https://inside.vermont.gov/projects/AOT%20MATS%20IR/Shared%20Documents/IR%20Artifacts%20from%20AOT/IR%20Meeting%20Artifacts/UPGRADE TEST MATS New module_release.docx		

Tool & Process							
T7	Support and Maintenance is Task based and only for 14 days after delivery and acceptance.	There is no warranty or ongoing support and maintenance for the software	384	Address if the business case supports it.	<p>1. See #2 in T6.</p> <p>2. No Action Needed: The State owns the code & has developed expertise in-house to support it, so AOT doesn't need to spend State money on a Maintenance Agreement with Delcan. If/When needed, AOT can contract with Delcan for specific maintenance tasks.</p>	No	
Data Management							
D1	With respect to Vision ERP, the data exchange file format is in flux and not defined. This issue is not unique to MATS and is indicative of a bigger issue and lack of a Master Data Model within the SoV	Payroll will not be met	576	stand up or re-allocate local VT environment	<p>Closed: The issue has been addressed and no further action is needed. The data exchange file format has been defined, is no longer in flux, & is in production.</p>	No	

Governance, Risk & Compliance							
G3	Lack of current and up-to-date COOP and/or D/R Plan	MATS is unusable during an emergency 'event'	504	Revise plan	<p>1. <u>AOT Pre-Contract Action:</u> AOT has a COOP Plan that will be updated to include MATS. As part of this plan a Risk Assessment for MATS will be performed & included in the plan.</p> <p>2. <u>AOT Pre-Contract Action:</u> AOT is working to define the DR and COOP. AOT DR infrastructure is in place. Next step is to test with MATS to see if infrastructure can support MATS or if additional hardware may be needed. Due to ERP implementation, MATS DR testing may not take place until July and the COOP finalized sometime in August/September timeframe. Failover procedures will be included.</p> <p>3. <u>AOT Future Commitment/No Pre-Contract Action:</u> AOT will create & implement a plan for annual testing of the COOP & DR plan with regard to MATS.</p>	<p>https://inside.vermont.gov/projects/AOT%20MATS%20IR/Shared%20Documents/IR%20Artifacts%20from%20AOT/IR%20Meeting%20Artifacts/OPS_MATS%20Security_DR_Plan-06102013.docx</p>	<p>https://inside.vermont.gov/projects/AOT%20MATS%20IR/Shared%20Documents/IR%20Artifacts%20from%20AOT/IR%20Meeting%20Artifacts/FW%20AOT%20COOP%20-%20Final.msg</p>

Governance, Risk & Compliance							
G7	Lack of compliance with respect to DII Security Standards policy	Security Breach	448	Implement policies and procedures with Vendor	<p>1. AOT Pre-Contract Action: Complete a Business Case & Cost Model specifically for the new Delcan contract and the enhancements being pursued as part of this contract.</p> <p>2. Comply with the Password Policy (See A3).</p>	https://inside.vermont.gov/projects/AOT%20MATS%20IR/Shared%20Documents/IR%20Artifacts%20from%20AOT/IR%20Meeting%20Artifacts/Copy%20of%20Draft%20PreliminaryLifecycleCostAnalysis.xlsx	https://inside.vermont.gov/projects/AOT%20MATS%20IR/Shared%20Documents/IR%20Artifacts/Draft%20Business-Case.doc
G9	Lack of Independent Review for each TASK/SOW	Value and Best practice. Current process appears to circumvent intent of IR.	360	Program Project and Portfolio Management representation from DII	<p>AOT Pre-Contract Action: Complete a 5 Year Road Map for MATS</p>	https://inside.vermont.gov/projects/AOT%20MATS%20IR/Shared%20Documents/IR%20Artifacts%20from%20AOT/IR%20Meeting%20Artifacts/VT_MA%20TriStateExpenditureTS_RoadmapForMATS_Delcan_06032013.docx	https://inside.vermont.gov/projects/AOT%20MATS%20IR/Shared%20Documents/IR%20Artifacts%20from%20AOT/IR%20Meeting%20Artifacts/Copy%20of%20Roadmap_Priority_Listing_v0_0327.xls

Appendix F - IR Disposition of Risk Considering Final Submissions

As described, the following tables reflect the disposition of the risk items including recommendations based on the strategy and additional submissions by VTrans.

Each of the following six (6) Risk items are still open and require action for closure and include:

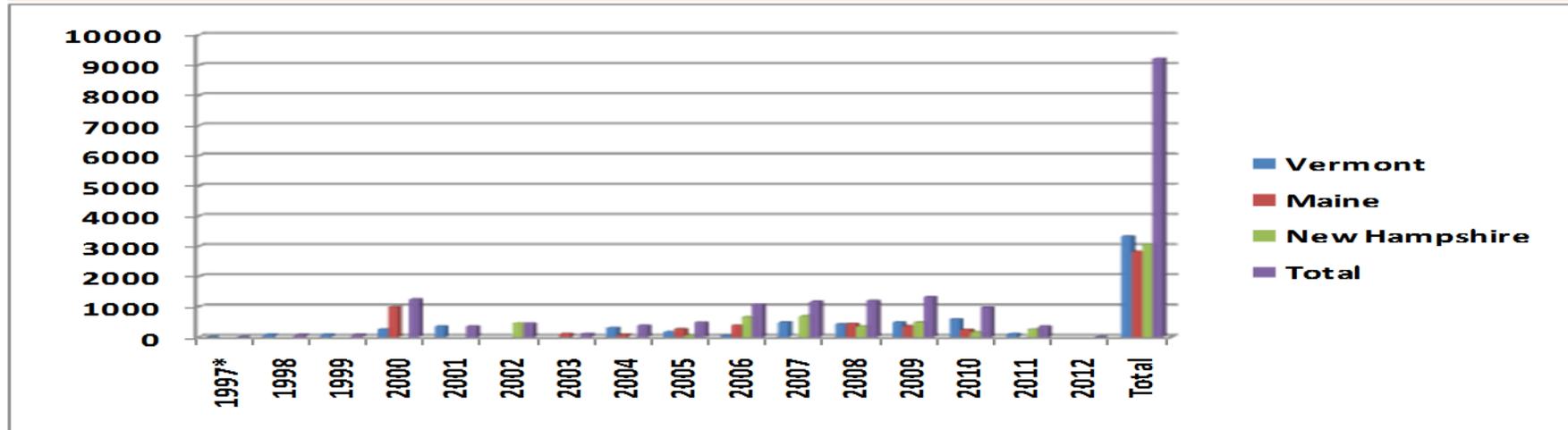
1. Lack of enforcement by code for password policies.
2. Testing and User Acceptance Testing is performed in Delcan environment
3. Support and Maintenance is Task based and only for 14 days after delivery and acceptance.
4. Lack of current and up-to-date COOP and/or D/R Plan
5. Lack of compliance with respect to DII Security Standards policy
6. Lack of Independent Review for each TASK/SOW

ID	Item/Function Issue	Potential Risk Event	PRN	Coeur Recommendation	AOT Risk Strategy	Coeur Final IR Disposition 06/27/2013
Architecture & Technology						
A3	Lack of enforcement by code for password policies. This should include access logs for MATS	Security Breach	720	Add rules and functionality to code. Issue password guidelines to users. OR SSO using Active Directory	AOT Pre-Contract Action: AOT will implement the MATS Release that includes Password enforcement. AOT will provide the release related documentation for this enhancement as evidence that it meets DII's Password Policy.	Disposition: Not Acceptable. Does not exist in current release. Recommendation: Proceed with funding to provide the fix in the next release, Re-evaluate and document for compliance.
Tool & Process						
T6	Testing and User Acceptance Testing is performed in Delcan environment	Local bugs, issues, and incidents	512	Stand up or re-allocate local VT environment	1. AOT Future Commitment/ No Pre-Contract Action Needed: AOT performs their own testing on all enhancements. Documentation will now be kept by AOT on test scenarios and results for each new MATS release. 2. AOT Pre-Contract Action: Contract currently only allows 14 days to identify issues with a new release. This does not allow adequate time for testing. AOT will negotiate an extension for this provision to 30 days.	Disposition: Not Acceptable. Testing needs to follow structured scripts with documentation that the testing was performed. Recommendation: Non-critical to MATS function. DII to proceed and implement existing UAT procedures from Vision/Vantage procurement and implementation.
T7	Support and Maintenance is Task based and only for 14 days after delivery and acceptance.	There is no warranty or ongoing support and maintenance for the software	384	Address if the business case supports it.	1. See #2 in T6. 2. No Action Needed: The State owns the code & has developed expertise in-house to support it, so AOT doesn't need to spend State money on a Maintenance Agreement with Delcan. If/When needed, AOT can contract with Delcan for specific maintenance tasks.	Disposition: Non-acceptable. At this time there was no new contract provided Recommendation: Non-critical to MATS function. DII to proceed, with the condition that 14 days is changed to 30 days in the contract to be let.

ID	Item/Function Issue	Potential Risk Event	PRN	Coeur Recommendation	AOT Risk Strategy	Coeur Final IR Disposition 06/27/2013
Data Management						
D1	With respect to Vision ERP, the data exchange file format is in flux and not defined. This issue is not unique to MATS and is indicative of a bigger issue and lack of a Master Data Model within the SoV	Payroll will not be met	576	stand up or re-allocate local VT environment	Closed: The issue has been addressed and no further action is needed. The data exchange file format has been defined, is no longer in flux, & is in production.	
Governance, Risk & Compliance						
G3	Lack of current and up-to-date COOP and/or D/R Plan	MATS is unusable during an emergency 'event'	504	Revise plan	<p>1. AOT Pre-Contract Action: AOT has a COOP Plan that will be updated to include MATS. As part of this plan a Risk Assessment for MATS will be performed & included in the plan.</p> <p>2. AOT Pre-Contract Action: AOT is working to define the DR and COOP. AOT DR infrastructure is in place. Next step is to test with MATS to see if infrastructure can support MATS or if additional hardware may be needed. Due to ERP implementation, MATS DR testing may not take place until July and the COOP finalized sometime in August/September timeframe. Failover procedures will be included.</p> <p>3. AOT Future Commitment/No Pre-Contract Action: AOT will create & implement a plan for annual testing of the COOP & DR plan with regard to MATS.</p>	<p>Disposition: Non-acceptable. At this time there was no DR Test submitted, the plan was incomplete and work in process. The Risk Assessment was incomplete and consisted of 2 items</p> <p>Recommendation: Non-critical to steady state system operations. DII to proceed with contract and work with Vtrans to develop a COOP plan and testing in-line with the State and Critical Systems.</p>
G7	Lack of compliance with respect to DII Security Standards policy	Security Breach	448	Implement policies and procedures with Vendor	<p>1. AOT Pre-Contract Action: Complete a Business Case & Cost Model specifically for the new Delcan contract and the enhancements being pursued as part of this contract.</p> <p>2. Comply with the Password Policy (See A3).</p>	<p>Disposition: Non-Acceptable. Limited and incomplete submissions with respect to Business case, Cost Model, and MATS Roadmap as required by statute.</p> <p>Recommendation: Non-critical to system Operation. Work with DII and DII/CIO to produce plan and documentation in line with expectations.</p>
G9	Lack of Independent Review for each TASK/SOW	Value and Best practice. Current process appears to circumvent intent of IR.	360	Program Project and Portfolio Management representation from DII	AOT Pre-Contract Action: Complete a 5 Year Road Map for MATS	<p>Disposition: Non-acceptable at this time as there was no roadmap to reconcile with the entire expenditure</p> <p>Recommendation: Non-Critical to business operation of MATS. Work with DII/CIO to reconcile.</p>

Appendix F – Project Costs To Date

MATS Expenditures by State by Year																	
	1997*	1998	1999	2000	2001	2002	2003	2004	2005	2006	2007	2008	2009	2010	2011	2012	Total
Vermont	551*	75	75	250	350			300	166	50	480	420	485	580	100		3,331
Maine				990			99	75	260	375		425	360	240			2,824
New Hampshire						449			47	650	685	350	475	155	250		3,061
Total	551*	75	75	1,240	350	449	99	375	473	1,075	1,165	1,195	1,320	975	350	0	9,216



Note: 1997* value of \$551K is the value of the original Vermont contract that did not yield a workable system; numbers are not included in the totals.

Note: 2009 values reflect the tasks processed under both the initial and the current Tri-State Contracts.