Board Meeting

Independent Assessments Briefing

February 24, 2016

Olivier Jullian, North Highland
Adam Gaydosh, Anitian

Agenda

1. Assessment Professionals
2. Project Management
3. System Integration
4. System Security
5. Summary

Assessment Professionals

- ✓ North Highland -- eFare Project Management Assessment
  - Global consulting firm providing industry experts in end-to-end program delivery, methodology and leadership

northhighland.
WORLDWIDE CONSULTING

- ✓ Anitian -- eFare System Integration and Security Assessment
  - Consultants serving thousands of companies on all matters security, governance and privacy.

ANITIAN
INTELLIGENT INFORMATION SECURITY

Project Management Assessment

Evaluation Methodology

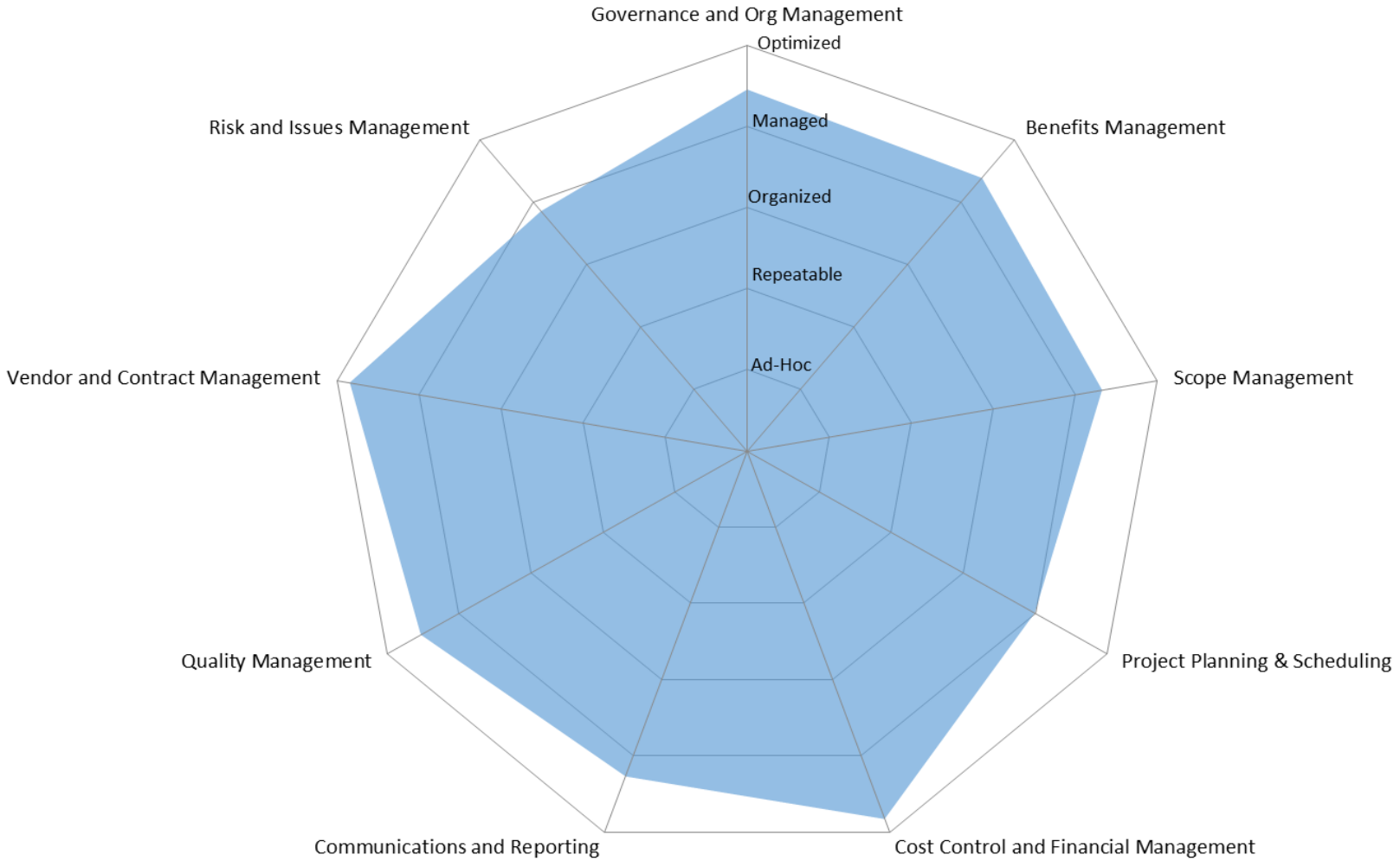
- ✓ Governance & Organization Management
- ✓ Benefits Management
- ✓ Scope Management
- ✓ Project Planning & Scheduling
- ✓ Cost Control and Financial Management
- ✓ Communications & Reporting
- ✓ Quality Management
- ✓ Vendor and Contract Management
- ✓ Risk & Issues Management

Key Observations

Interviewed over 40 stakeholders involved in implementation

- ✓ Team was engaged, responsive and transparent
- ✓ Project is well-run with consideration for careful execution
- ✓ High-level of confidence in eFare success
- ✓ Leadership and sponsorship team involvement is commendable

Project Health Scorecard



Key Risks, Issues and Actions

- Lacks comprehensive project management plan with integrated dependencies
  - ✓ Comprehensive plan existed; staff since updated it to include GlobeSherpa integrated schedule
- Missing overall quality assurance plan and lead
  - ✓ QA staff existed and operated in the role; staff is now officially assigned
- Internal communications solid; some gaps identified
  - ✓ Forwarding Board Report to extended stakeholders; created monthly dashboard
- Formal risk/issue management not inclusive of all risk areas
  - ✓ While a comprehensive risk management plan existed, staff has since included discussions with extended stakeholders

Project Management Assessment Summary

- ✓ Project team engaged and transparent
- ✓ Well-balanced project management across all categories
- ✓ No major areas of concern
- ✓ Key Risks, Issues addressed 30 days after assessment

System Integration & Technical Assessment

Alignment with Best Practices

RISK
(PROJECTED)

Strengths	Opportunities
• Very effective use of security technologies at point of sale to encrypt payment data and minimize impact on compliance • Robust coordination between vendors and design components • The existing PCI security control framework can be easily extended to apply to eFare systems	• Components of the architecture are not yet designed or finalized; most notably, the details concerning encryption and key management • Vendor development processes do not include consistently formal, robust security reviews • System and network security controls are not currently deployed on pre-production systems

System Integration

System Integration

Technical Design and Integration Assessment Tasks:

- ✓ System Design
- ✓ Transaction Volumes
- ✓ Data Security
- ✓ Disaster Recovery
- ✓ Design Documentation
- ✓ Hosting

Findings

Task	Description
System Design	• Finalized components demonstrate robust design; open or incomplete design areas should be addressed before final acceptance.
Transaction Volumes	• Potential bottlenecks exist between validator cellular network usage and calls to back-office components
Data Security	• The GlobeSherpa-hosted environment is not fully dedicated to Tri-Met production eFare system

Findings

Task	Description
Disaster Recovery	• The Data Warehouse implementation used for report generation is not fully redundant. • Existing continuity of operations plan (COOP) is robust but needs to be updated for eFare • Data backup process not efficiently integrated with virtual server system. • Restoration of certain components currently dependent on vendor assistance
Design Documentation	• System designs are very well documented in most cases • Open and recently designed components require additional documentation before final acceptance.
Hosting	• Some vendor-hosted environments need to be formally aligned with industry or regulatory security standards

System Security

System Security

System Security Assessment Project Tasks:

- ✓ Compliance Review
- ✓ Network Security
- ✓ Data Security
- ✓ Physical Security
- ✓ Application Security
- ✓ IT Policies
- ✓ Test Plans

Findings

Task	Description
Compliance Review	• Validator encryption scheme aligns with payment card industry guidelines. Obtain formal approval of the scheme from TriMet's merchant bank. • Some vendor products are currently undergoing industry standard security validation. Deploy validated software versions to eFare environment.
Network Security	• Approach for remote vendor access to production environment should be finalized prior to commissioning of this environment. eFare network is not currently segmented by trust level of systems. Additional network segmentation should be implemented prior to commissioning of production system.
Data Security	• Formal system security standards should be developed and deployed to eFare servers. • Encryption key management process should be formalized for all databases and vendors.

Findings

Task	Description
Physical Security	• Inconsistent level of formality in physical system access control across different groups. A consistent approach should be defined and enforced. Fare media handling procedures should be updated and enforced for eFare.
Application Security	• Enforce patch management to all systems regardless of vendor support • Work with vendors to ensure that important application updates to commercial product are implemented in the eFare software branch. • Formalize secure software development and change management practices for all application development
IT Policies	• A responsibilities matrix should be created to define specific management responsibilities for each vendor
Test Plans	• Complete all test plans and include security testing

System Integration and Security Summary

- ✓ TriMet has demonstrated thorough due diligence in defining the business, IT and security requirements for eFare and in coordinating with their vendors.
- ✓ Not all aspects of the design have been finalized, but the most critical components have
- ✓ Some of TriMet's design exceeds industry best practices.
- ✓ The gaps in best practices are relatively minor and easily addressable at this stage of the project