Alaska Land Mobile Radio
Risk Management Plan

Version 1w

June 27, 2019

Table of Contents

Document Revision History

Name	Date	Reason for Changes	Version
Shafer, Sherry	12/19/2008	Approved by the User Council - Final.	2
Shafer, Sherry	2/11/2010	Annual review/update. Approved by the User Council - Final.	3
Shafer, Sherry	2/16/2011	Annual review/update. Approved by the User Council - final.	4
Shafer, Sherry	6/82012	Annual review/update; approved by the User Council - final.	5
Shafer, Sherry	6/4/2013	Annual review/update; approved by the Operations Management Office - final.	6
Shafer, Sherry	6/16/2014	Annual review/update. Approved by the Operations Management Office - final.	7
Shafer, Sherry	6/18/2015	Annual review/update. Approved by the Operations Management Office - final.	8
Shafer, Sherry	6/16/2016	Annual review/update. Approved by the Operations Management Office - final.	9
Shafer, Sherry	6/29/2017	Annual review/update. Approved by the Operations Management Office - final.	10
Shafer, Sherry	6/5/2018	Annual review/update. Approved by the Operations Management Office - final.	11
Shafer, Sherry	6/27/2019	Annual review/update. Approved by the Operations Management Office - final.	12

Definitions and Acronyms

Alaska Federal Executive Association (AFEA): federal government entities, agencies and organizations, other than the Department of Defense, that operate on the shared ALMR system infrastructure.

Alaska Land Mobile Radio (ALMR) Communications System: the ALMR Communications System, which uses but is separate from the State of Alaska Telecommunications System (SATS), as established in the Cooperative and Mutual Aid Agreement.

Alaska Municipal League: a voluntary non-profit organization in Alaska that represents member local governments.

Change Control Board (CCB): includes representatives from each of the major stakeholders who evaluate requested changes to the ALMR System, and identify possible impacts and the risks associated with them.

Cooperative Agreement: the instrument that establishes ALMR and sets out the terms and conditions by which the System will be governed, managed, operated and modified by the Parties signing the Cooperative and Mutual Aid Agreement.

Department of Administration (DOA): a State of Alaska (SOA) department that maintains the SOA Telecommunication System (SATS) and provides information technology (IT) and communications technical support to state agencies.

Department of Defense – Alaska: Alaskan Command, US Air Force and US Army component services operating under United States Pacific Command and United States Northern Command.

Executive Council: the ALMR Executive Council which is made up of three voting members and two associate members representing the original four constituency groups: the State of Alaska, the Department of Defense, Federal Non-DOD agencies (represented by the Alaska Federal Executive Association), and local municipal/government (represented by the Alaska Municipal League and the Municipality of Anchorage).

Member: a public safety agency including, but not limited to, a general government agency (local, state or federal), its authorized employees and personnel (paid or volunteer), and its service provider, participating in and using the System under a Membership Agreement.

Municipality of Anchorage (MOA): the MOA covers 1,951 square miles with a population of over 300,000. The MOA stretches from Portage, at the southern border, to the Knik River at the northern border, and encompasses the communities of

Girdwood, Indian, Anchorage, Eagle River, Chugiak/Birchwood, and the native village of Eklutna.

Operations Management Office (OMO): develops recommendations for policies, procedures, and guidelines; identifies technologies and standards; and coordinates intergovernmental resources to facilitate communications interoperability with emphasis on improving public safety and emergency response communications.

State of Alaska (SOA): the primary maintainer of the SATS (the State's microwave system), and shared owner of the System.

State of Alaska Telecommunications Systems (SATS): the State of Alaska statewide telecommunications system microwave network.

System: the ALMR Communications System, as established in the Cooperative Agreement, and any and all System Design/System Analysis (SD/SA) and System Design/System Implementation (SD/SI) documents.

System Management Office (SMO): the team of specialists responsible for management of maintenance and operations of the System.

User: an agency, person, group, organization or other entity which has an existing written Membership Agreement to operate on ALMR with one of the Parties to the Cooperative and Mutual Aid Agreement. The terms user and member are synonymous and interchangeable.

User Council (UC): the User Council is responsible for recommending all operational and maintenance decisions affecting the System. Under the direction and supervision of the Executive Council, the User Council has the responsibility for management oversight and operations of the System. The User Council oversees the development of System operations plans, procedures and policies under the direction and guidance of the Executive Council.

1.0 Introduction

Risk management is the systematic process of identifying, analyzing and responding to risks. It includes maximizing the probability and consequences of positive events, as well as minimizing the probability and consequences of adverse events.

2.0 Scope

The Alaska Land Mobile Radio (ALMR) risk management processes include:

- Risk management planning – how to approach and plan risk management activities
- Risk identification – determining which risks might affect the System and documenting their characteristics
- Quantitative risk analysis – measuring the probability and consequences of risks and estimating their implications
- Risk response planning – developing procedures and techniques to enhance opportunities and reduce threats
- Risk monitoring and control – monitoring residual risks, identifying new risks, executing risk reduction plans and evaluating their effectiveness throughout the System life cycle

In order to plan for, identify, analyze, respond to and mitigate risks, you must understand what a risk is. A risk is an event or condition that, if it occurs, has a positive or negative effect. A risk has a cause and a consequence, and risk identification should include aspects of the physical, political and social/cultural environment. These aspects may even contribute to the risk, such as an unexpected windfall, or conversely, poor management practices or over dependency on external participants who cannot be controlled.

Risks include both threats to the overall objectives and, also, opportunities to improve on those objectives. Known risks are those that have been identified and analyzed, and it may be possible to plan for them. Although unknown risks cannot be managed, they may be addressed by applying a general contingency based on experience with previous projects/undertakings, as well as best practices taken from other similar organizations.

Organizations normally perceive risk as it relates to threats to their success. Some risk may be acceptable, but only if it balances with the benefit that may be gained. To be successful, all stakeholders must be committed to addressing risk management.

3.0 Methodology

The process used in the creation of the initial ALMR Risk Management Plan followed the guidelines adopted by the Project Management Institute[1].

Development of the initial plan began with a review of available documentation and included risks previously identified by ALMR personnel. This was followed by a series of internal discussions and one-on-one interviews. Identified risks were documented and then analyzed to determine which risks could be accepted and which would be included in the initial plan.

This plan incorporates additional risks identified outside of the initial steps taken, including those perceived for the immediate future. For each of the risks included in the risk response plan, an expanded risk description and a risk mitigation strategy was created.

Risk management for ALMR includes monitoring and control of the processes necessary to manage risks throughout the lifecycle of the System.

4.0 Identified Risks

This section contains a list of risks that were identified and are being tracked. They are not listed in priority order, but simply grouped under an appropriate category. Identified risks are rated from low to disastrous, reflecting the impact of the risk to the ALMR System and interoperability among member agencies. Risk probability is measured on the degree of likelihood that it will occur and is rated low to very high.

Risk mitigation strategies and an escalation matrix were developed, which outline the steps to be taken to protect the System from the lowest to the highest level of possible impact from the identified risk. The level of impact on the ALMR System and interoperability, as a whole, was taken into consideration.

As the probability increases/escalates, the impact rating may also escalate. The risk's impact rating is determined by its overall effect on ALMR.

The assigned risk severity number is derived by multiplying the probability of occurrence by the impact of occurrence, and then normalizing the result for all possible results on a 0 to 100 scale for easy relative reference. The scoring system is designed so that increasing scores denote increasing risk severity. The overall risk score is converted to a percentage and assigned a severity color, which highlights the current areas of greatest concern.

[1] Located at www.pmi.org

Projected Impact/Probability/Rating of Identified Risks

Identified Risk	Probability	Impact	Risk Severity
Technical Risks			
System (physical)	**Moderate**	**Disastrous**	**50**
Individual sites	**High**	**High**	**47**
System updates	**High**	**Moderate**	**28**
System performance	**Moderate**	**Moderate**	**28**
Subscriber equipment	**Moderate**	**Moderate**	**19**
Dispatchers not adequately trained	**Low**	**High**	**16**
Users not adequately trained	**Moderate**	**High**	**31**
System administrators/technologists not adequately trained	**Low**	**High**	**16**
Political Risks			
Agencies elect not to participate	**Moderate**	**High**	**31**
Consortium fails	**High**	**Disastrous**	**75**
Conflicting priorities of the different agencies	**High**	**Disastrous**	**75**
Legislative changes	**High**	**Disastrous**	**75**
User expectations	**Low**	**High**	**16**
Lack of senior management support	**High**	**Disastrous**	**75**
Funding Risks			
Sufficient funds cannot be approved for System updates	**High**	**High**	**47**
Sufficient funds cannot be obtained for subscriber equipment (initial costs /replacement costs)	**High**	**High**	**47**
Sufficient funds are not available for on-going O&M of the System	**High**	**Disastrous**	**75**
Funds are allocated and then withdrawn for other priorities	**High**	**Disastrous**	**75**
Agencies elect to not participate due to costs	**Low**	**High**	**16**
Management Risks			
Poor allocation of time and resources	**Low**	**Moderate**	**9**
Poor use of management disciplines	**Low**	**High**	**16**
Inadequate communication	**Moderate**	**High**	**31**
Loss of key personnel	**Moderate**	**High**	**31**

Identified Risk	Probability	Impact	Risk Severity
External Risks			
Acceptance by stakeholders	**Moderate**	**High**	**31**
Changing stakeholder priorities	**High**	**Disastrous**	**75**
Natural disasters, conflicts, terrorism	**Moderate**	**Moderate**	**28**
Changes in the O&M contracts	**Moderate**	**High**	**31**
Unexpected state windfall	**Low**	**Low**	**3**

Probability weighted score		Impact weighted score		Severity Color
Low (1-25%)	**1**	**Low**	**1**	**Low**
Moderate (26-50%)	**2**	**Moderate**	**3**	**Moderate**
High (51-75%)	**3**	**High**	**5**	**High**
Disastrous (76 - 100%)	**4**	**Disastrous**	**8**	**Disastrous**

The impact of an occurrence is deemed more critical in the final result than the probability of occurrence. This methodology assumes that an event with a low probability of occurrence, and a disastrous impact, would still be relatively important, while an event with a higher probability of occurrence, but a low impact, would be less significant.

The formula used to derive the final score is:

$$\frac{\text{(Probability Score) X (Impact Score) X 100}}{\text{(Maximum Probability Score X (Maximum Impact Score)}}$$

5.0 Mission Strategies and Response Summaries

Specific risks and the suggested mitigation strategies are listed in the following table.

Risk Area	Specific Risk	Mitigation Strategy	Owner	Response Summary
Technical Risks				
System risk (physical)	There is the possibility that ALMR will not continue to work as anticipated due to technical difficulties and inappropriate use of technology.	Rely on knowledgeable technical personnel for solutions and operational expectations planning. Ensure contracts are in place to protect the System from exposure to failure.	SMO Cooperative Partners	Motorola technical solutions
Individual Site Risk	There is the possibility that an individual site will fail due to any number of reasons including manmade/natural disasters, technical difficulties, a lack of proper maintenance and inappropriate use of technology.	Contingency plans should be put in place to protect the System from exposure to failure due to unanticipated constraints/events.	SMO Cooperative Partners	Motorola technical solutions Contingency plans
System updates	The System may fail due to unanticipated technical/ compatibility problems that surface as software advances.	Rely on the experience and expertise of knowledgeable technical personnel to ensure proper handling/deploying of technology in a manner consistent with the life cycle of the System.	SMO Cooperative Partners	Motorola technical solutions
System performance	The possibility exists that the System may not perform as specified for any number of unknown/unanticipated technical reasons relating to the actual performance observed.	Perform testing against data benchmarks throughout the System life cycle to uncover any potential issues.	SMO	Motorola technical solutions Annual periodic maintenance inspections
Subscriber equipment	There may be instances where particular subscriber equipment	Return individual equipment to the manufacturer for repair/	Agencies	Acceptance Test Procedures

Risk Area	Specific Risk	Mitigation Strategy	Owner	Response Summary
	fails, or fails to perform as anticipated.	replacement. Have sufficient warranties, additional maintenance support plans or spare equipment to ensure interruptions are minimized and continuous operation is not jeopardized.	SMO	Warranties Spares Maintenance contracts
Dispatchers not adequately trained	Dispatch personnel training will not be completed in a timely manner, is inadequate or is not up to date.	Ensure that training is a priority and training dates are met. Personnel should regularly attend refresher courses or test on a recurring basis.	Agencies	Training plan
Users not adequately trained	Subscriber users will not be trained properly on equipment features and functions.	Ensure there is a detailed training plan and personnel are proficient at operating the equipment.	Agencies	Training plan
System administrators/ technologists not adequately trained	The System may be fully functional and operating but System administrators or technologists may not be available or properly trained.	Ensure there is a detailed Training Plan for System administrators and technologist. Provide upgrade or refresher training, as required.	SMO	Contracted system management Training plan
Political Risks				
Agencies elect not to participate	Agencies may become discouraged and elect not to participate. This may be motivated by various factors including changing political priorities, continued funding problems, unrealistic expectations or other unanticipated and unavoidable developments.	Effective communications can minimize confusion and bring problems to light before they become critical. Management should ensure agencies are actively engaged and that their concerns and situations are understood and dealt with in a timely manner.	OMO UC EC	Senior leadership champions

Risk Area	Specific Risk	Mitigation Strategy	Owner	Response Summary
Consortium fails	There is always the possibility that the consortium could fail, for any number of political, tactical or management reasons.	The best defense against a complete failure comes back to an effective communications plan and the active support of management at all levels. These are probably the two key tools that can be used to stack the odds in favor of stakeholder buy-in and a resulting success.	OMO UC EC	Allied support letters Senior leadership champions
Conflicting priorities of the different agencies	Agencies may agree on the need for common communications protocols, but may be thwarted from common goals by the realities of individual agency priorities.	Individual agency champions should ensure that their agency's participation does not get buried or left behind due to shifting agency needs. Constant communication and feedback will be a vital tool in this effort.	UC Agencies	Leadership champions
Legislative changes	The reality of life everywhere, both political and personal, is that legislative changes are always a potential source of good or bad, progress or slippage, and support or opposition.	Legislative changes, short of employing lobbying efforts and legislative vigilance, cannot be influenced. Keeping the System and its merits in the public eye may minimize legislative impacts.	UC EC Cooperative partners	Public relations
User expectations	Unrealistic user expectations can kill an initiative or doom an on-going project to failure. If stakeholders do not understand the project, and they have not bought-in with realistic expectations, sooner or later, they will lose interest and	Ensure user expectations are realistic and effectively manage the System. Provide clear and continuous communication. Be clear on capabilities in meeting the user's needs and why their involvement is critical. Ensure agency buy-in by constant support	OMO/SMO UC EC	Outreach/Education

Risk Area	Specific Risk	Mitigation Strategy	Owner	Response Summary
	withdraw their support/depart.	and communication.		
Lack of senior management support	Of all of the political risks, this is probably one of the most critical. Without senior management support, or worse, with senior management opposition, the System may fragment and fail.	The best tool to ensure senior management support is to provide clear and continuous communication. If senior management does not feel like the needs of their agencies are being met, they will not be supportive. If they do not support the System, they will not promote the needed funding.	UC EC Cooperative partners	Status meetings/reports
Funding Risks				
Sufficient funds cannot be approved for System updates	There may be any number of reasons why funds may not be available for updates, regardless of the desire of agencies to participate in what they know is a valuable and worthwhile endeavor.	There are four variables that can typically be adjusted: scope, schedule, cost and quality. If money runs out, you can decrease the scope thereby decreasing the cost; stretch the schedule to slow expenditures and hope for additional funding later; lower the quality and save cost or live with a sufficient, but not optimal, product. All of these strategies should be evaluated in the event that funding falters.	Agencies EC Cooperative partners	Adequate budget planning
Sufficient funds cannot be approved for subscriber equipment	Regardless of the support and enthusiasm exhibited by the member agencies/potential member agencies, there may not be adequate funding to provide/replace subscriber	The sooner equipment funding needs are addressed, the better. Budget for initial purchases/ replacements should be a priority for agencies. Available grant opportunities should be vigorously	Agencies UC	Adequate budget planning Grant opportunities

Risk Area	Specific Risk	Mitigation Strategy	Owner	Response Summary
	equipment.	explored, as well.		
Sufficient funds are not available for on-going O&M of the System	The System was implemented successfully, but it is possible the on-going operation and maintenance (O&M) may prove too onerous for the stakeholders to bear.	It is critical that all stakeholders realize the full extent of on-going O&M costs. Assuming that these costs are realistically computed, agencies can knowledgeably plan for O&M of their components and, where necessary, obtain additional funding via supplemental budgets/add-ins.	Agencies EC Cooperative partners	Adequate life-cycle planning
Funds are allocated and then withdrawn for other priorities	There is always the possibility that competing priorities will siphon off projected/available funds.	Good management, communication, sponsors, and realistic expectations can be used to keep the System going and provide ammunition to fight for interoperable communications when other priorities surface. If funds cannot be obtained through supplemental budgets, the services provided may need to be reduced.	Agencies EC Cooperative partners	Adequate life-cycle planning Reduce scope
Agencies elect to not participate due to cost	It is extremely likely many agencies will withdraw from the System if there is an associated cost.	Continue to illustrate the need for, and benefit of, interoperability to public safety, first responder agencies. Encourage them to communicate this to the public they serve, their State representatives and, ultimately, their respective funding bodies.	Agencies UC EC Cooperative partners	Adequate life cycle planning Alternate funding sources Usage fees

Risk Area	Specific Risk	Mitigation Strategy	Owner	Response Summary
Management Risks				
Poor allocation of time and resources	One of the main purposes of management is to ensure that valuable time and resources are not wasted. Regardless of the talent that is brought to any project, it may still get off track or even fail if that talent is not managed. Some acceptable and appropriate methodology must be adopted, followed, and enforced.	Projects/updates should be managed according to PMI guidelines. Implementation plans will map how the process will proceed; roles and responsibilities tables should map out the operational phase. Project schedules will be one of the major control tools.	OMO/SMO UC EC Cooperative partners	Project schedules Implementation plans Gantt charts
Poor use of management disciplines	Regardless of the management methodology employed, poor use of the selected management disciplines will result in exposure to failure.	Manage expectations to ensure System goals, maintenance and status is appropriately communicated to all stakeholders. Standardized configuration management principles should be implemented to ensure that the process is reliable, objective and independent of personalities, track changes to ensure users are not impacted.	OMO/SMO UC EC Cooperative partners	Enhance management skills Hire experts Quality assurance/quality control Configuration management Change control procedures
Inadequate communication	The greatest organization in the world is useless if no one knows anything about it, or worse, if it is created and then ignored, or not managed properly.	Management is critical tool to ensuring that outreach and education occurs on several levels. This can be done utilizing several methods. Publicizing goals and objectives from the beginning with periodic updates utilizing standard	OMO/SMO UC EC	Implement communications methods System status reports System metrics

Risk Area	Specific Risk	Mitigation Strategy	Owner	Response Summary
		agreed-upon System metrics.	Cooperative partners	
Loss of key personnel	Loss of key personnel could place the System at risk. This is a common problem for all organizations.	Possible solutions include assignment of roles and responsibilities, cross training of key personnel, and the maintenance of a contract relief pool. A productive and rewarding work environment will also help to foster team spirit and morale.	OMO/SMO Agencies	Cross-train personnel Employee pool Esprit de corps
External Risks				
Acceptance by stakeholders	Regardless of the obvious advantages of interoperability, or even the potential for mandated actions, there may be some stakeholders who do not accept the product, or who make uninformed decisions based on hearsay.	Stakeholders should be actively involved in shaping the goals and on-going O&M of the System and are much more likely to continue their support if they feel that they truly do have an ownership stake in the project. Comprehensive communication and strict implementation of agreed upon actions can ensure stakeholder support, cooperation and participation.	EC Cooperative partners	Cooperative agreement Clear goals and expectations
Changing stakeholder priorities	Regardless of the excellence of System management expertise, there may be some stakeholders whose support waivers based on changing agency priorities. After all, their primary loyalty is to their	Full and open communication with stakeholders is critical given the differences of agency environments. It is also critical to have active support within upper echelons to ensure that agencies	Agencies UC	Enlist executive sponsors and champions Life cycle planning/management

Risk Area	Specific Risk	Mitigation Strategy	Owner	Response Summary
	agency and the successful pursuit of that agency's missions.	can be influenced to complete their commitments despite changing priorities.	EC Cooperative partners	
Natural disasters, conflicts, terrorism	Regardless of how much pre-planning takes place, there will always be disasters, natural or man-made, and unforeseeable incidents.	Effective disaster recovery, incident response planning and contingency planning can be adopted to mitigate the effects of disastrous external events.	OMO/SMO UC EC	ICS responses Contingency planning Disaster drills
Changes in the O&M contracts	The possibility exists that the price of future contracts may increase; additional personnel may be required and future updates needed.	As budgetary conditions change, adjustments can be made so that operations/maintenance can continue on a reduced scale, if needed.	OMO/SMO UC EC Cooperative partners	Adequate life-cycle planning Budget projections
Unexpected state windfall	It might not seem like an unexpected State windfall would adversely affect progress but good news can sometimes be just as disruptive as bad news.	Criticality of the strong support cannot be overstated. In good times and in bad, the sponsor ensures that the stakeholders are focused on the goals and not diverted by new and unexpected circumstances.	EC Cooperative partners	Unfunded requirements list Action plan

6.0 Monitoring and Control

Risk monitoring and control is the process of keeping track of the identified risks, monitoring residual risks, identifying new risks, ensuring the execution of risk plans and evaluating their effectiveness in reducing risk. Risk monitoring and control is recorded through the use of metrics that are associated with implementing contingency plans. Risk monitoring and control is an on-going process throughout the life of the System. Risks will change as a System matures; new risks may develop or anticipated risks may lessen or disappear.

Good risk monitoring and control processes provide information that assists with making effective decisions in advance of the risk occurring. Communication to stakeholders is needed to periodically assess the acceptability of the level of risk. A risk owner should be assigned to each identified risk.

Risk monitoring determines if:

- Responses have been implemented, as planned
- Response actions are as effective as expected, or if new responses should be developed
- Exposure has changed from its prior state
- Proper policies and procedures are in place and being followed
- Risks have arisen that were not previously foreseen

Risk control may involve choosing alternative strategies, implementing a contingency plan or taking corrective action. The risk response owner should periodically report on the effectiveness of the plan, any unanticipated effects, and any mid-course correction needed to mitigate the risk.

Inputs into risk monitoring and control include:

- Risk Management Plan
- Risk Response Plan
- Communications such as issue logs, action item lists, change requests, System status reports, etc.
- Additional risk identification and analysis

The following tools and techniques are recommended for risk monitoring and control.

6.1.1 Risk Reviews

Risks should have regularly scheduled reviews as ratings and prioritization may change during the life cycle of a System. Any change may require additional qualitative or quantitative analysis.

6.1.2 Additional Risk Response Planning

If a risk emerges that was previously not anticipated in the risk response plan, or its impact on objectives is greater than expected, the planned response may not be adequate. It will be necessary to perform additional response planning to control the risk.

6.1.3 Output

The following outputs are products of the risk monitoring and control process:

6.1.3.1 Workaround Plans

Workarounds are ad hoc responses to emerging risks that were previously unidentified or accepted. Workarounds must be properly documented and implemented.

6.1.3.2 Corrective Action

Corrective action consists of implementing a contingency plan or workaround.

6.1.3.3 Change Requests

Implementing contingency plans or workarounds frequently results in a requirement to institute a change. The result is a System Change Request issued by the UC and managed by the Change Control Board. Specific details concerning the change request process are located in the System Change Request Management Policy and Procedure 400-3.

7.0 Updates to the Risk Response Plan

Risks may or may not occur. Risks that do occur should be documented and evaluated. Implementation of risk controls may reduce the impact or probability of recurrence. Risk rankings must be reassessed so that new, important risks may be properly controlled. Previously identified risks that are no longer a threat should be closed during the annual review/update of the Risk Response Plan.

8.0 Risk Records Management

Use of a records repository for collection, maintenance and analysis of data gathered and used in risk management will assist managers throughout the organization and, over time, help form the basis of a lessons learned program.

9.0 Conclusion

The User Council shall be responsible for the formal approval of the Risk Management Plan and any substantial revisions hereafter.