Risk Management Plan
for
Lattice QCD Research Program Extension III

Unique Project (Investment) Identifier: 019-20-01-21-02-1032-00

Operated at
Brookhaven National Laboratory
Fermi National Accelerator Laboratory

for the
U.S. Department of Energy
Office of Science and High Energy

Version 0

June 5, 2019

PREPARED BY:
Josephine Fazio, FNAL

CONCURRENCE:

June 5, 2019

__________________________ __________________________________

William Boroski
LQCD-ext III Contract Project Manager

Date

LQCD-ext III Risk Management Plan
Change Log

Version No.	Description	Effective Date
0	Risk Management Plan updated to reflect LQCD-ext III operations model; removed reference to JLab.	May 9, 2019

Table of Contents

1 Introduction

This document describes the risk management plan for the Lattice Quantum Chromodynamics Computing Research Program Extension III (LQCD-ext III) for the period FY2020 through FY2024. This document and the associated Risk Register[i] are LQCD-ext III Controlled Documents.

The LQCD-ext III research program (hereafter LQCD) is an extension of the LQCD-ext II project, which is funded through FY2019. It will support the continued acquisition and operation of institutional cluster computing resources located at Brookhaven National Laboratory (BNL) and Fermi National Accelerator Laboratory (FNAL). BNL and FNAL provide facilities and infrastructure that deliver the mid-scale computing required by the LQCD program. They also provide computing professionals to plan, design, deploy, and operate the computing systems.

2 Overview of the Risk Management Plan

2.1 Purpose and Objective

As defined in the LQCD-ext III Project Execution Plan (PEP), the Integrated Project Team (IPT) views risk management as an ongoing activity that is accomplished using a formalized plan to identify, analyze, mitigate and monitor the risks that arise during program execution. LQCD established its risk management plan during the early stages of the project using the guidelines set forth in Chapter 14 of DOE Publication M 413.3-1[ii], Project Management for the Acquisition of Capital Assets. The current revision is based on the guidance provided in the Guide to the Project Management Body of Knowledge[iii] and the OMB Circular Number A-11 Part 7 Capital Programming Guide[iv].

As defined in these references, risk is a measure for the potential of failing to achieve overall objectives within the defined scope, cost, schedule and technical constraints. The purpose of this document is to describe 1) how the LQCD IPT plans to manage and minimize risks; and 2) document actions to be put in place in a timely and consistent manner in case of an occurrence.

The LQCD risk management strategy is to avoid risk as much as possible by identifying possible risks and devising methodologies for managing them. LQCD risks are focused in two areas:

a. Enclave-based risks associated with the hosting laboratories. Computing systems used by LQCD remain under the jurisdiction of the hosting laboratories as a part of their General Enclaves. Each host laboratory is responsible for implementing risk management plans that address enclave-based risks such as security, privacy, and business continuity. Enclave-based risk management methods are addressed in laboratory-specific documents and mitigated by laboratory-specific technologies.

b. Program-based risks associated with overall program execution.

2.2 Responsibility

The final responsibility for risk management rests with the Contract Project Manager (CPM), who takes appropriate measures in consultation with the LQCD IPT, the USQCD Executive Committee, and other stakeholders. Designated Site Managers at each site are responsible for managing sitespecific risks. Notwithstanding, effective risk management is an iterative, multi-step process that requires the continued involvement of all project members.

3 Risk Assessment

Since a key requirement is to deliver high performance computing that optimizes performance/price ratio for LQCD computing, it is necessary to accept certain levels of risks to achieve the scientific objectives of the program. Eliminating risk entirely is not a viable option so the LQCD IPT embraces a "risk aversion to a moderate degree" approach. The strategy is to reduce risk to an acceptable level by effectively using management and planning to mitigate risks as they arise. The LQCD risk management process is integrated with the technical plans and PEP and various control mechanisms are in place to manage residual risks.

3.1 Risk Assessment Planning

The annual planning process includes identifying and reviewing risks, determining probability of occurrence and degree of impact, and developing risk mitigation strategies. Annual planning considers all factors affecting operations and technical performance.

Technical plans that support LQCD include annual acquisition plans and alternative analyses documents, both of which contain descriptions and potential impacts of risks associated with annual hardware acquisitions.

Identified risks are documented in the LQCD Risk Register, which also contains records of outcomes of the qualitative risk assessment. A change management process, outlined in the LQCD PEP, is in place to manage significant changes required to address realized risks.

3.2 Risk Management Execution

Throughout the program lifecycle, the LQCD IPT periodically evaluates risk by using management tools and metrics, including:

- Bi-weekly site manager meetings
- Monthly project completion status reports
- Monthly financial status reports
- Monthly technical accomplishment reports
- Change requests and their approvals or rejections
- Periodic review of risks identified in the Risk Register.

Existing risks and mitigation strategies are reviewed and updated as necessary. Whenever a new risk is identified and receives a risk rating of medium or high, a risk mitigation strategy is developed and implemented. Any associated scope, cost or schedule changes required by mitigation actions is handled according to the Project Change Control procedure described in the PEP.

4 Risk Identification

The Risk Register workbook contains a tab "Risk Register" that contains the list of identified risks, along with the following attributes:

- Risk ID – unique identifier across all risks
- Risk Area – for risk categorization, one of:
  - Cost, Schedule, Technology; Security, Service
- Risk Title – Short description of the risk for reporting
  - No more than 3 lines at current field width.
- Description – Long description of the risk (narrative)
- Probability of Occurrence – one of:
  - High, Medium, Low
- Impact of Occurrence – one of:
  - Severe, Moderate, Low
- Risk Rating – numerical value based on Risk Rating Table
  - Rating Value = Probability Value * Impact Value
- Risk Priority – one of: (based on Risk Rating value)
  - High, Medium, Low
- Risk Status – one of:
  - Active – risk condition has occurred, so the risk has become a real issue.
  - Exists – risk condition has not occurred
  - Retired – risk condition is no longer considered worthwhile tracking
- Creation Date (date)
- Last Review Date (date)
- Next Review Date (date) – driven by review frequency or earlier date chosen by IPT
- Last Change (narrative, should include date)
- Mitigation Strategy (narrative)
- Notes (narrative)

Detailed information regarding each identified risk is recorded in the narrative fields in the Risk Register.

5 Risk Analysis

Each identified risk is analyzed for the probability and impact of occurrence. Individual ratings for probability and impact are assigned based on the values shown in Table 1. A risk rating is then derived by multiplying probability and impact values; risk ratings are shown in Table 2. Finally, each risk is assigned a priority based on the risk rating value. Risk priority is used to drive the level of planning and frequency of monitoring required for the risk.

Table 1: Risk Probability and Impact Values

Probability	Value	Impact	Value
High	0.75	Severe	0.9
Medium	0.50	Moderate	0.5
Low	0.25	Low	0.1

Table 2: Risk Rating Matrix (with Risk Priority color coding)

		Impact		
		Severe	Moderate	Low
Probability	High	0.675	0.375	0.075
	Medium	0.450	0.250	0.050
	Low	0.225	0.125	0.025

Table 3: Risk Prioritization Table

Risk Priority	Rating Low Value	Rating High Value	Risk Planning Level	Risk Plan Location	Risk Review (Minimum) Frequency
1 - High	0.500	1.000	Detailed Risk Plan	Separate Document	At least monthly
2 - Medium	0.150	0.500	Modest Risk Plan	Risk Register	At least quarterly
3 - Low	0.000	0.150	Minimal Risk Plan	Risk Register	At least annually

6 Risk Handling

The primary risk handling strategy is to avoid risks where possible by developing sound plans based on reasonable assumptions and then validating those assumptions with the Executive Committee, Scientific Program Committee, and other technically qualified individuals.

LQCD also uses various risk minimization tools and techniques, such as:

System and subsystem prototyping

Benchmarking using modeling and simulation

Formal and informal technology assessments

Quality control and system validation

Alternative acquisition analysis

System and subsystem level risk assessments including prioritization

Continuous monitoring of technical and financial performance measures

Establishing various surety measures including security and disaster recovery measures

Risks are categorized into one of five major "risk areas": Technology, Cost / Schedule (following DOE guidelines), Security (computer security and privacy issues), and Service (business/service continuity and disaster recovery issues). General mitigation strategies for each major risk area are described below.

6.1 Technology Risk Mitigation

The major technical concern for the LQCD program is the annual delivery of computing capabilities, expressed in Tflop/s-yrs. Prior to the beginning of the 5-year research program, the CPM develops a 5-year computing performance plan that defines the anticipated computing resources that will provided to the research program by each host laboratory. During program execution, the CPM refines and updates the computing plan prior to the beginning of each fiscal year. The CPM works with the EC and SPC to refine computing needs for the coming year, and with each host laboratory Site Manager to confirm computing resource availability. Consequently, LQCD can reliably predict prior to the beginning of any fiscal year the Tflop/s-yrs that will be delivered in the fiscal year. This allows for detailed planning, by the Scientific Program Committee, of allocations to scientists for access to these computing resources.

In any given year, one or both host laboratories may decide to bring on additional computing capacity. This may occur through the expansion of existing systems or the acquisition and deployment of a new system using a new technology. Since either scenario involves hardware acquisition planning, procurement and deployment, there are cost, schedule and technical risks associated with these activities. Since LQCD and each host laboratory have extensive experience in the deployment of new systems, cost and schedule overruns are of low to moderate probability with moderate impact. Schedule estimates are based on publicized release dates (e.g., “roadmaps”) provided by manufactures for hardware components and the delivery dates given by the third-party vendors and integrators who are subcontracted for hardware purchases. Since LQCD must rely on state-of-the-art technologies to deliver the highest possible computing power within budget, it is often advantageous to wait for the most advanced technologies, for example, processor and switching technologies, promised by the manufacturer. However, if the manufacturer fails to deliver on publicized dates, the schedule may slip, or the project may have to procure existing technology at lower performance.

There is also a technical performance risk associated with new deployments of advanced technologies, as it is possible that a new system will not deliver performance at expected levels. By tracking and benchmarking new products available in the market, prior to executing an acquisition, technical risks are of low probability. Moreover, impact is low to moderate as any new system will only be a fraction of the overall hardware portfolio. Even if a new system does not quite meet performance expectations, the impact on overall computing delivered will be marginal.

6.2 Cost Risk Mitigation

Because LQCD funding is directly affected by approval of the federal budget, there may delays in the availability of funds due to factors such as Continuing Resolutions. To mitigate this risk, a portion of operating funds are set aside and carried forward to cover one month of operations at the beginning of a fiscal year.

Memoranda of Understanding (MOUs) are established between the LQCD and each host laboratory prior to the start of each fiscal year. Documented in each MOU are the agreed-upon costs for specified levels of delivered computing and storage resources, as well as a modest level of funding for Site Manager support. Costs are tracked through the year and corrective actions are taken as necessary to prevent cost overruns.

Staffing issues may also affect the project cost. Since only a small number of technical staff members are directly associated with LQCD, there is a low to moderate probability of risk associated with the loss of key project members. However, the impact of the loss of key personnel can be high in terms of full release of new computing systems to the scientific community and annual technical delivery. To mitigate this risk, as much as practical, LQCD staff members at two or more of the host sites participate in the prototyping, planning, and execution of each major system acquisition. Cross-training of system administration duties is encouraged whenever possible. This ensures that LQCD maintains historical knowledge and technical expertise in at least several individuals.

6.3 Schedule Risk Mitigation

Schedule risk is tied to technology and cost risks, as previously discussed. If hardware availability does not keep up with technology roadmaps or if cost becomes higher than forecast, the ability to deliver projected computing cycles will be affected. The general risk mitigation strategies in this area consists of 1) staying abreast of technical advances and timing of new releases; and 2) optimizing the timing of annual procurements, from both a cost and schedule perspective, to deliver the most Tflop/s-yrs possible from all available resources at hand.

6.4 Security Risk Mitigation

Security management of the computing facilities hosted by each laboratory is administered by the physical and cyber-security infrastructure established by that laboratory. The LQCD-ext III Security Plan for a set of computing equipment within an enclave is updated and approved whenever any new equipment is added to an enclave. Each laboratory keeps its Certification and Accreditation (C&A) documents up to date. The hosting laboratory also performs required scans and other monitoring and assessments. Since LQCD computing facilities comprise special purpose equipment protected by strong security system protocols, external access by unauthorized users is unlikely. No private, personal or otherwise, information may be retained on LQCD computer facilities.

6.5 Service Risk Mitigation

Since delivering high performance computing to the USQCD user community is a critical objective of this program, LQCD has considered disaster recovery planning from its inception. LQCD takes advantage of the institutional disaster recovery plans for the computing centers at each of its host laboratory sites. These plans are reviewed periodically.

The most valuable data products produced are the vacuum gauge configuration data files, which may require in aggregate many Tflop/s-yrs. of computing. These files are stored redundantly at multiple locations, including two or more of FNAL, TJNAF, BNL, NERSC, TACC, ORNL, the ALCF, and LLNL. The principal investigator for each computational project executed on LQCD resources is responsible for safeguarding the data products produced by his or her scientific project.

Following standard government policy, the equipment at each facility is not insured against disasters, though the standard safety protections provided by each laboratory assure as much as possible the protection of the equipment. The distributed nature of the meta-facility partially mitigates the risk of natural disasters, allowing for critical scientific calculations to be moved from one host site to another in the event of a sustained outage.

7 Risk Monitoring

The Risk Register is reviewed and updated whenever a new risk is identified, a risk is determined to no longer affect the project, or a change in the environment is detected that may affect existing risks or risk plans. In steady state, absent such changes, a graded approach is used for risk monitoring based on the risk priorities and schedules presented in Table 3.

Risks assigned a “1 – High” priority receive the most attention in risk planning. They are reviewed at least monthly and whenever the IPT believes there is a need to review the risk, as tracked in the Next

Review Date field. They will have a detailed risk plan developed and maintained in a separate document outside of the Risk Register (a document reference is stored in the Risk Register).

Risks assigned a “2 – Medium” priority will receive moderate attention in risk planning. They will be reviewed at least quarterly, and whenever the IPT believes there is a need to review the risk, as tracked in the Next Review Date field. They will have modest risk plans which will be captured in the narrative fields of the Risk Register.

Risks assigned a “3- Low” priority will receive the least attention in risk planning. They will be reviewed annually, and whenever the IPT believes there is a need to review the risk, as tracked in the Next Review Date field. They will have minimal if any risk plans, often just noting in the Risk Register that the risk has been identified and accepted.

The LQCD Program Office reviews the Risk Register monthly for entries that may be affected by changes in the environment or which have an upcoming “Next Review Date” to prepare the IPT for a risk item review. The LQCD IPT will also take advantage of the annual DOE Progress Review to review the long-term risk management plans with the reviewers. The LQCD Risk Management Plan is updated annually.

8 List of Acronyms

Acronym	Definition
ALCF	Argonne Leadership Computing Facility
BNL	Brookhaven National Laboratory
C&A	Certification and Accreditation (computer security)
CCB	Change Control Board
DOE	Department of Energy
FNAL	Fermi National Accelerator Laboratory (a.k.a. Fermilab)
IPT	Integrated Project Team
LLNL	Lawrence Livermore National Laboratory
LQCD	Lattice Quantum Chromodynamics
NCSA	National Center for Supercomputing Applications
NERSC	National Energy Research Scientific Computing Center
ORNL	Oak Ridge National Laboratory
QCD	Quantum Chromodynamics
TACC	Texas Advanced Computing Center
Tflop/s	Teraflops per second. 1 teraflop = 10^12 floating point operations
Tflop/s-yr	Computing delivered by 1 TFlop/s sustained for one year
TJNAF	Thomas Jefferson National Accelerator Facility (a.k.a. JLab)

[i] Risk Register for the LQCD-ext III project

[ii] DOE G 413.3-7 Risk Management Guide (9-16-08)

[iii] A Guide to the Project Management Body of Knowledge (PMBOK® Third Edition), Project Management Institute

[iv] OMB Circular Number A-11 Part 7 Capital Programming Guide V2.0 (2006) Appendix 5