NASA Space Science Data Coordinated Archive

Archive Assurance Plan

15 September 2016

Approved by:

_____

Edwin Grayzeck
Project Manager, Solar System Exploration Data Services Office, GSFC

_____

William Knopf
Program Executive, Planetary Science Division, NASA HQ

NSSDCA Archive Assurance Plan

APPENDICES

NSSDCA Archive Assurance Plan

Change History Log

Version Number	Description of Changes and Affected Sections	Approved By	Approved Date
01	Initial document release	E. Grayzeck	2016-09-15

NSSDCA Archive Assurance Plan

1 Purpose and Scope

This Archive Assurance Plan (AAP) describes how the NASA Space Science Data Coordinated Archive (NSSDCA) will identify, analyze, track, communicate, and mitigate risks to the achievement of its performance requirements. This plan is based on requirements in NPR 8000.4A (2014) NASA Agency Risk Management Procedural Requirements Section 3.1.

2 Stakeholders

NSSDCA stakeholders and their functions with respect to NSSDCA archive assurance activities are identified in the table below. Personnel associated with the stakeholder roles are identified in Appendix A.

Stakeholder	Function
Program Executive, Planetary Science Division, NASA HQ	Executive oversight
Project Manager	Executive authority, chair of the NSSDCA Configuration Control Board
Project Scientist	Long-term preservation
Configuration Control Board	Evaluate defined risks relative to performance requirements, track risk monitoring, ensure appropriate mitigation, AAP custodian
NSSDCA Technical Staff	Systems administration and security, data ingest, archival storage, long-term preservation, applications development, database installation, upgrades, maintenance, task supervisors

3 Performance Requirements

The NSSDCA's high-level performance requirements are identified in the following table. Risks relevant to each performance requirement are assessed qualitatively with a subjective evaluation risk of risk probability and impact. Little quantitative assessment is currently performed at NSSDCA. Quantitative risk assessment is typically more time-consuming than qualitative risk assessment and frequently requires assessment tools. A number of NSSDCA performance requirements could be assessed quantitatively as well as qualitatively. In the future, NSSDCA will implement quantitative assessment as available resources permit. Appendix B explicitly addresses safety, technical, cost, and schedule risks and relates them to these performance requirements.

Performance Requirement	Qualitative Risk Assessment	Potential Quantitative Risk Assessment
Facility and infrastructure maintenance	√	
Systems administration	√	√
Systems development	√	√
Digital data ingest	√	√
Digital archival storage	√	√
Data dissemination	√	√
Analog archival storage	√	√
Long-term preservation	√	√

4 NSSDCA Approach to Archive Assurance

4.1 Archive Assurance Processes

NASA has adopted two complimentary processes to for risk management: Risk-Informed Decision Making (RIDM) and Continuous Risk Management (CRM). The RIDM process uses performance measures along with other considerations to make risk-informed decisions. RIDM has six steps organized into three parts.

Part 1 Identification of Alternatives
- Step 1 – Understand Stakeholder Expectations and Derive Performance Measures
- Step 2 – Compile Feasible Alternatives

Part 2 - Risk Analysis of Alternatives
- Step 3 – Set the Framework and Choose the Analysis Methodologies
- Step 4 – Conduct the Risk Analysis and Document the Results

Part 3 - Risk-Informed Alternative Selection
- Step 5 – Develop Risk-Normalized Performance Commitments
- Step 6 – Deliberate, Select an Alternative, and Document the Decision Rationale

CRM is an iterative and adaptive process to monitor and mitigate risk, using communication, deliberation, and documentation. The five steps in the CRM cycle are:

Identify	Identify risks by identifying scenarios with adverse consequences.
Analyze	Estimate the likelihood and consequence of risk
Plan	Decide what is tracked, thresholds for corrective action, and appropriate control measures
Track	Monitor observable performance
Mitigation	Exercise appropriate corrective actions and control measures

The NSSDCA approach to archive assurance is one based on the RIDM and CRM processes that is commensurate with the deep archive's level of staffing, resources, and funding.

4.2 The Configuration Control Board

The NSSDCA Configuration Control Board (CCB) is the executive entity within the NSSDCA. The project manager is the chair person of the CCB with decision making authority. Other CCB members have an advisory role and are responsible for ensuring that CCB decisions are implemented. These advisory members include task supervisors responsible for communications between the CCB and NSSDCA technical staff. The CCB may delegate responsibility to other stakeholders within the NSSDCA.

The CCB establishes the performance measurement requirements identified in section 3. These requirements are periodically reviewed by the CCB and amended as needed to insure that they accurately reflect the expectations of NSSDCA's external stakeholder and provide appropriate services to the NSSDCA's user community.

4.3 Risk Identification

The CCB identifies risks related to performance requirements and verifies the likelihood and consequence analysis of each risk. Corrective actions and control measures are re-evaluated as well. Recognized risks and their mitigation measures as determined by the CCB are listed in Appendix B. At regular intervals, the CCB reassesses those risks and updates the list as needed. When the list is revised, other NSSDCA stakeholders will be notified.

4.4 Risk Elevation

Risks to NSSDCA performance requirements could include risks that are mitigated at the NSSDCA, risks that are mitigated by an external entity, or risks that are accepted because the risk involved is not severe enough to warrant the added cost it would take to avoid that risk. Decisions to elevate risks to an external entity are made by the jointly by the CCB chair person and the Program Executive.

4.5 Risk Monitoring and Mitigation

Technical staff members continuously monitor NSSDCA performance and will typically be first to identify a risk occurrence. For each risk occurrence technical staff initiates predefined mitigation measures, as identified in Appendix B. Staff members may identify a previously unrecognized risk or an improvement to an existing mitigation measure. In those cases the improvement or newly identified risk is forwarded to the CCB for consideration.

4.6 Risk Reporting

Risk-related communication between NSSDCA and external entities is performed by the CCB chair person. At regular intervals **TBD** the CCB will produce a risk preparedness report to be

conveyed by the CCB chair person to the Program Executive. Internally, technical staff report risk occurrences to the CCB as they are identified and mitigated. The CCB chair person and the Program Executive shall decide if other external entities (e.g. data providers) shall be notified of NSSDCA of risk occurrences.

5 Other Affected Entities

NASA Active Archive Discipline Nodes and other organizations that have Memorandum of Understanding with NSSDCA may be affected by risk occurrences at the deep archive.

6 References

[1] NASA Agency Risk Management Procedural Requirements, NASA/NPR 8000.4A, NASA Goddard Space Flight Center, Greenbelt, MD, 2008 (revalidated January 2014; expires December 2019).

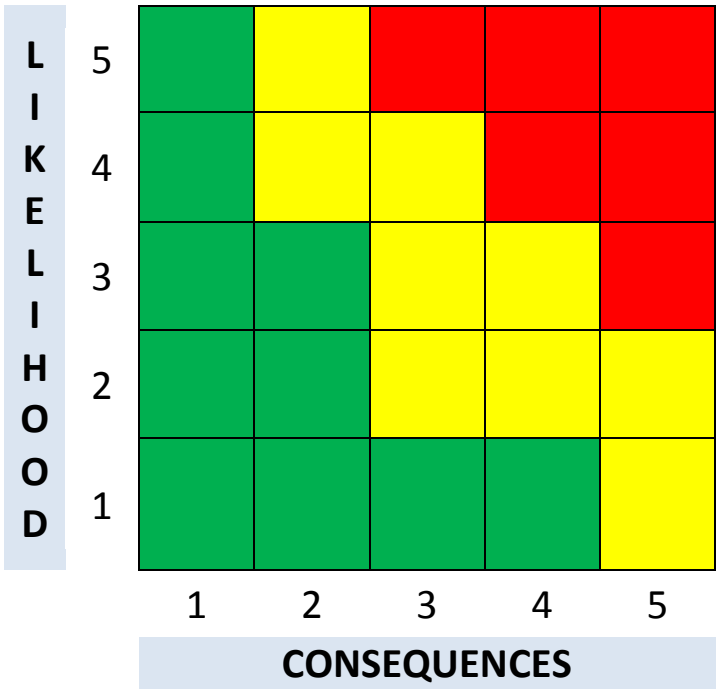
[2] NASA Risk Management Handbook, NASA/SP-2011-3422, Version 1.0, NASA Headquarters, Washington, D.C., November 2011.

7 Acronym List

CRM	Continuous Risk Management
NASA	National Aeronautics and Space Administration
NSSDCA	NASA Space Science Data Coordinated Archive
RIDM	Risk-Informed Decision Making

NSSDCA Archive Assurance Plan
Appendix A – NSSDCA Risk Identification and Mitigation

The NSSDCA risk matrix is used to determine the risk levels based on occurrence probability and consequence severity.



High risk

Moderate Risk

Low Risk

Consequence Categories				
1	2	3	4	5
Negligible or no impact to achievement of performance requirements	Minor impact to full achievement of performance requirement	Moderate impact. Minimal achievement of requirement is possible with margin.	Major impact. Minimal fulfillment of requirement is possible.	Minimal fulfillment of performance requirement is not possible.

Likelihood	
1	Rare
2	Unlikely
3	Possible
4	Likely
5	Certain

NSSDCA Archive Assurance Plan

1-2, Low; 3, Medium; 4-5 High

Facility and Infrastructure Maintenance Risks Qualitative assessment	Likelihood	Consequence Severity	Threat level	Mitigation Measures
Fire	1	5	Medium	Copies of data maintained at remote location
Water (Flood/Sprinkler System	2	5	Medium	Copies of data maintained at remote location
Earthquake (significant damage)	1	5	Medium	Copies of data maintained at remote location
Earthquake (moderate damage)	2	4	Medium	Copies of data maintained at remote location
Earthquake (limited damage)	2	1	Low	Copies of data maintained at remote location
Other structural	3	3	Medium	Copies of data maintained at remote location
Electrical surges	4	3	Medium	Have critical systems on UPS
Electrical blackouts	2	3	Medium	Have critical systems on UPS
Temperature	3	3	Medium	Daily environmental checks
Humidity	3	3	Medium	Daily environmental checks
Staffing level decrease	3	3	Medium	
Essential personnel – no redundancy	3	5	High	
Loss of institutional knowledge	4	3	Medium	
Staff error	3	2	Medium	
Single source dependency: products and services	2	4	Medium	

1-2, Low; 3, Medium; 4-5 High

Systems Administration Risks Qualitative assessment	Likelihood	Consequence Severity	Threat level	Mitigation Measures
Fraud and theft	2	3	Medium	Identify and minimize access to personal information Identify most valuable physical assets and minimize access

Staff sabotage	1	5	Medium	Minimize elevated privileges Keep copies of data, metdata and software in a secure location
Hacking	4	4	High	Adhere to prescribed security measues
Digital theft	1	2	Low	Adhere to prescribed security measues
Malware	4	5	High	Adhere to prescribed security measues
Threats to personal privacy	1	2	Low	Minimize access to personal information
System vulnerability: vendor software				
System vulnerability: in-house software				

1-2, Low; 3, Medium; 4-5 High

Systems Development Risks **Qualitative assessment**	**Likelihood**	**Consequence Severity**	**Threat level**	**Mitigation Measures**
Loss of code repository integrity	2	5	Medium	Regular backups of code repository stored off-site
Code obsolescence	3	4	Medium	Identify dependencies and continuously move to new versions, testing and then modifying code as needed.
Lack of development tools	2	4	Medium	
Single source dependency: tools and products				

1-2, Low; 3, Medium; 4-5 High

Digital data ingest Risks **Qualitative assessment**	**Likelihood**	**Consequence Severity**	**Threat level**	**Mitigation Measures**
Internet connectivity	4	4	High	
Equipment malfunction	3	5	High	Current maintenance agreementes

Staff error	3	3	Medium	Establish SOP for digital data ingest
Single source dependency: tools and products				
Insufficient resources to accommodate data				

1-2, Low; 3, Medium; 4-5 High

Digital archival storage Risks **Qualitative assessment**	**Likelihood**	**Consequence Severity**	**Threat level**	**Mitigation Measures**
Degradation of data on magnetic media	5	5	High	Media refreshed on 8 year cycle using contemporary technology.
Degradation of data on non-magnetic media				
Physical damage to magnetic media	5	5	High	
Magnetic damage to media	3	3	Medium	Store in clean temperature-stable environment away from electronic equipment
Digital media obsolescence	5	5	High	Media refreshed on 8 year cycle using contemporary technology.
Digital data corruption	5	5	High	Media refreshed on 8 year cycle using contemporary technology. Checksums used for data integrity.
Insufficient resources to accommodate data				

1-2, Low; 3, Medium; 4-5 High

Data Dissemination Risks **Qualitative assessment**	**Likelihood**	**Consequence Severity**	**Threat level**	**Mitigation Measures**
Insufficient resources to stage data	2	2	Low	

Analog Archival Storage Risks Qualitative assessment	Likelihood	Consequence Severity	Threat level	Mitigation Measures
Damage to analog material	3	5	High	Establish SOP for handling and storage of analog materials
Analog material degradation	2	2	Low	Establish SOP for handling and storage of analog materials

1-2, Low; 3, Medium; 4-5 High

Long Term Preservation Risks Qualitative assessment	Likelihood	Consequence Severity	Threat level	Mitigation Measures
Digital data format obsolescence	3	5	High	Conversion of old data
Digital data reduced usability to community	5	1	Medium	
Metadata corruption	5	3	High	
Metadata reduced usability over time	5	1	Medium	