FERMILAB INDEPENDENT ASSESSMENT REPORT FORM

Fermilab Independent Assessment Report	
Assessment Number & Title: 10-IA-QA-006 CD-WAN/MAN	**Version:** A07
Date(s) of Assessment: 7/29/10 – 8/3/10	
Performing Organization: Office of Quality & Best Practices	
Assessed Organization(s): Computing Division, Wide-Area Networking Group	

Report content

This report contains the following sections:

- Assessment Activities & Scope
- Scope Limitations
- Activities Reviewed Within this Assessment
- Description of the Implementation & Effectiveness of Observed Activities
- Conclusions
- Findings, Observations, & Recommendations
- Commendable Practices

Assessment Activities & Scope:

The implementation & effectiveness of controls for wide-area networking administrative and technical activities were examined via interview and document review relative to selected requirements of the Integrated Quality Assurance (IQA) and Fermilab Integrated Contractor Assurance (FICAP) program.

Scope Limitations:

The scope of this assessment was limited to those activities or services associated with the Fermilab wide-area network (WAN) perimeter and metropolitan area network (MAN) systems managed and/or maintained by the Wide-Area Network Group within the Computing Division. Within the MAN, only the two local hubs for which Fermilab has maintenance responsibilities were addressed.

Activities Reviewed Within this Assessment:

- Specification & acquisition of equipment and services
- Oversight of initial vendor setup & configuration
- Oversight & monitoring of routine system operation
- Response to manual or automated alerts relating to system performance

Description of Implementation & Effectiveness of Observed Activities:

<u>Assessments:</u>

Quality and contractor assurance requirements for assessments are met within the WAN group. Annual

self assessments required by the DOE via OQBP are conducted by the group leader. Examples of these completed self assessments are included as Files 01 & 02. FESHM-mandated ES&H assessments are not conducted specifically within the activities of this group because of the scope and nature of the WAN activities. Corrective actions identified as necessary within WAN activities are managed through the CD Service Desk through completion.

Design:

There are no hardware design activities within the WAN group per se. Performance requirements for proposed systems are provided to suppliers who provide commercial, off-the shelf (COTS) equipment meeting those requirements. Work Smart standards are not used; there are none relevant to WAN activities.

Design configuration is managed through the ITIL process in place within CD. An example of an approved, closed change request form is attached (File 03). This specific example documents the review and approval of a request to relocate an FNAL hub, part of the MAN. Direction on the determination of formal change request approval requirements is provided by a "Networking Change Risk Classification Guidance" document (File 04). This document provides five classifications of risk associated with changes and details the review and approval process to be followed for each.

Issues Management:

Requirements for issues management are met through the use of a division-wide system for assigning and tracking IT "incidents". Issues relating to WAN or MAN performance are referred to the CD Service Desk, which uses Service Desk "tickets" to refer issues for resolution, monitor resolution progress, and formally close issues when appropriate. Upon closure, the originator of the issue is notified of the closure, providing a verification mechanism for the originator. A copy of a closed incident ticket assigned to the WAN group is attached as File 05.

Incident trends are monitored by the Problem Manager and evaluated for potential escalation or broader remedial action as needed. Though no WAN/MAN incidents have been escalated to the Problem management system to date, a copy of a Problem Investigation report is attached as File 06. Because the division-wide Incident and Problem management systems are outside the scope of this assessment, a detailed review of the scope and effectiveness of these systems was not performed.

There have been no significant or reportable incidents within the WAN group, as defined under FESHM 3010. Reporting of such incidents would be forwarded to the division level through line management.

Performance:

Requirements for performance data collection and use are met. Four-year strategic plans are prepared for network operations with input from the WAN group. Annual tactical plans are developed based on this document by the WAN group. Examples of these plans are attached as Files 07 & 08. Areas requiring improvement identified in annual self assessments (Files 01 & 02) are reflected in the strategic and tactical plans as items to be addressed in the referenced timeframes.

Various network metrics (such as network traffic levels, reliability, and capacity) are collected on an automated basis by the systems. These metrics are also reflected in the self assessments and planning

documents above.

Program:

The requirements for the quality program specified in both the IQA and FICAP are met within the WAN/MAN operations. Performance goals for staff responsible for MAN and WAN activities within the WAN group are defined annually. Redacted examples are attached as Files 09 and 10. These goals provide individual-specific expectations, some common to the departmental-level goals defined in the strategic and tactical plans. The Computing Division organizational chart is maintained on the Division's website and a copy is attached as File 11. The WAN group reports through the Network & Virtual Services Department.

The application of a graded approach to process improvement is met through the use of a formal risk assessment process. The risk assessment supplements the divisional Cyber Security Protection Plan (CSPP) by addressing any additional risks specific to WAN/MAN operations not specifically addressed in the CSPP, such as "Unauthorized Network Functions". It also provides mitigation steps for the risks identified. A copy of the "Risk Assessment for the Wide Area Network System" is included as File 12. Additionally, specific controls beyond those specified in the CSPP are documented in the "Security Plan for the Wide Area Network System" (File 13). A "Contingency Plan for Network System" addresses back-up plans for residual risks beyond the controls established in the CSPP, the Risk Assessment, and the Security Plan. This Contingency Plan (File 14) addresses a worst-case scenario in which controls fail and back-up equipment must be brought in or relocated within the site.

Operation and maintenance of the MAN as a part of the broader of Energy Sciences Network (ESNet) is coordinated through a working group called the FNAL ANL network group (FANG). The flowdown of expectations and requirements for FNAL are specified in a memorandum of understanding (MOU) between Argonne National Laboratory and FNAL. A copy of this MOU is included as (File 15). Equipment procured is generally standard COTS items and custom performance requirements are not specified.

Quality Improvement:

The quality of the service that the group offers is effectively integrated into work through multiple, automated monitoring systems. In this small group, the responsibility for improvements in the quality of the service is largely informal, which appears to function effectively and efficiently. The staff feels empowered by management to propose changes to improve the level of the service whenever it is possible.

ES&H issues are not as prevalent in this group as in some others because of the nature of the work and the surroundings. Nevertheless, all were aware of the general importance of ES&H issues, and were familiar with a recent finding of a DC cord strain relief and how it was mitigated, attached as File 16. This issue was entered into and tracked to completion through ESHTRK, although not directly by the group members.

The interaction with the ITIL system and in particular the service desk ticket procedure offers good opportunities for improving quality and tracking it effectively.

Work Processes:

Work in the group is carried out in a well-defined, safe, and effective manner. The end product is well understood and achieved by application of clear, if often informal, procedures.

Maintenance of the hardware per se is accomplished by vendors under contract. Maintenance by the group consists mainly of monitoring routine operation and responding to automated reports, installation of routine upgrades of firmware and software, and testing failover capability for redundant systems. There is no schedule for these activities. They are normally accomplished in a reactive way as opportunities present themselves, rather than pro-actively scheduling planned preventive maintenance.

Property within the group is accounted for primarily through the formal Equip-DB database system. The group manager also maintains a more detailed, local record of equipment in a separate spreadsheet for use within the group. An excerpt is included as File 17.

Written procedures exist for some priority processes, particularly where they pertain to activities involving others outside the group. Examples include "Policy & Procedures for Authorized Access to Network Infrastructure & Services" (File 18) and "WAN Group Off-Hours Procedures" (File 19).

Conclusions:

The quality controls for the IQA and FICAP criteria selected for this assessment are met within the Wide Area Networking Group. The WAN and MAN systems are critically important, but they are largely automated operations requiring little human intervention. Controls for these systems are defined by the hardware configuration and software policies and the human input is primarily in the form of monitoring and testing of redundant systems. System metrics such as downtime and traffic loads are available from the systems themselves. These metrics are used in planning future improvements, as reflected in the strategic and tactical plans and risk assessments and mitigation strategies. The staff involved in overseeing and managing the WAN and MAN operations have extensive experience in their areas of responsibility and are well aware of the importance of their role in the overall mission of the laboratory and of the visibility of their operations to the lab staff and external users of the networks. The use of the Service Desk and ITIL process provide ample opportunities for quality improvement and assessment, and this tool is employed in the group.

Findings: None

Observations and Recommendations:

1. **Observation:** Definition of group and individual responsibilities
   Recommendation: Formal definition of individual and group responsibilities tied to divisional and departmental responsibilities and goals should be considered. There is no formal program requirement for such formal definition.

2. **Observation:** Scheduled testing of failover systems as a routine check / maintenance item
   Recommendation: Institute a standardized procedure for testing failover systems under conditions more closely simulating normal operating situations than is current practice. Such testing is now conducted primarily during "safe times", such as following system downtime.

3. **Observation:** Identification via graded approach of priority processes which may require documentation for performance by less experienced staff

Recommendation: Management should consider establishing criteria for formalizing procedures based on risk, complexity, scope of use, etc. Because of the size of the group and the automated nature of the groups' processes, it is not clear if documentation would serve to reduce process risks.

Titles and Names of Person Interviewed:

Vytautas Grigaliunas
Phil DeMar

Documents Reviewed:

2nd MAN Hub Business Case
ESnet CHI to build marked up redline 12-16-09 jcl(2)
FANG_MOU_final draft
FY09 wide-area network strategic plan
FY09 wide-area network tactical plan
FY10 combined department strategic plan
FY10 wide-area network tactical plan
FY2008_WAN_Self_Assessment
FY2009-WAN-Self-Assessment
MAN 2007 CHEP paper
MAN costs rev2b
MAN Schematic 2010-03-19(3)
MAN Topology 1-15-2010
QGSI Chicago Node Insertion - Channel AddMOP Rev 1.0
WAN overview talk
Wide-Area Network Contingency Plan
Wide-Area Network Risk Assessment
Wide-Area Network Security Controls

(See also "Attachments" section below)

Standards, Regulations, and Other Program Requirements Applied:

The specific criteria applied to this assessment were:

Fermilab Integrated Quality Assurance (IQA), Document 1001
- Chapter 1 - Program
- Chapter 3 - Quality Improvement
- Chapter 5 - Work Processes
- Chapter 6 - Design
- Chapter 9 - Assessments

Fermilab integrated Contractor Assurance (FICAP), Document 3901
- Chapter 1 - Program
- Chapter 4 - Assessments
- Chapter 5 - Performance
- Chapter 9 - Issues Management

Describe or List Any Other Assessment Methods Used: None

Corrective Action Plans Issued: None.

Assessors' Names (asterisk indicates team leader):

Kurt Mohr* - OQBP
Rod Walton - FESS

Submitted by: Kurt Mohr **Date:**

Distribution (Distribute to assessed organizations' management, OQBP head, and other interested parties):

B. Banerjee
W. Boroski
D. Coder
P. DeMar
V. Grigaliunas
M. Kaletka
J. Cotton
J. Grant
J. Heyes
R. Walton

Attachments:

File 01 FY2008 WAN Self Assessment.pdf
File 02 FY2009 WAN Self Assessment.pdf
File 03 Ciena Hub Change Request.pdf
File 04 Networking Change Risk Classification Guidance.pdf
File 05 Service Desk Incident Report INC44028.pdf
File 06 Service Desk Problem Report PBI090.pdf
File 07 FY2010 Combined Department Strategic Plan.pdf
File 08 FY2010 WAN Tactical Plan.pdf
File 09 Employee 1 Performance Goals MAN Support.pdf
File 10 Employee 2 Performance Goals WAN Support.pdf
File 11 CD Organization Chart.pdf
File 12 Wide-Area Network Risk Assessment.pdf
File 13 Wide-Area Network Security Plan.pdf
File 14 Wide-Area Network Contingency Plan.pdf
File 15 FANG MOU.pdf
File 16 ESHTRK Report for Ciena Hub Power Cable Stress Release.pdf
File 17 Property Office- WAN Group Active Assets.pdf
File 18 Policy & Procedure for Authorized Access to Network.pdf
File 19 WAN Off-Hours Procedures 100204.pdf