

FY08 Strategic Plan for Central Services (2008-2011)

(M. Kaletka, M. Leininger, J. Schmidt) 9/4/2008

Mission

Provide common central computing services which broadly underpin the Laboratory's Open Science and general technical and business missions.

Context and Assessment of Current State

The strategic plan for central services is guided by the [Computing Division Strategic Plan](#) and the strategic directions of the Laboratory program, and MOU's and SLA's established with other organizations, including internal Laboratory organizations (other Div's/Sec's). The strategic plan is also guided by cybersecurity guidance and directives imposed on the Laboratory by DOE.

The Computing Division provides a comprehensive set of central services which support the daily scientific and business functions of the lab (web, email, print, storage, database and application development, backup, etc.), the computing support infrastructure (patching, inventory, configuration mgmt, antivirus, authentication, metrics and accounting, etc.), and the computer security infrastructure (inventory, scanning, automated controls, etc.). While these services are available to essentially "all comers", not all parts of the Laboratory choose to use them, resulting in redundant expenditure of effort. In addition, several of the services have grown to be very complex, with limited depth of knowledge in the support groups (one or two "experts"), leading to concerns for future reliability.

Computer security is a well-planned and successful effort but is particularly impacted by reaction to the cybersecurity guidance and directives, and frequent short-deadline calls for information, flowing from various offices in DOE. These frequently do not take good account of the Open Science model of the Laboratory, so there is a constant struggle to minimize the impact on the Laboratory's scientific program, which draws effort away from managing the computer security program of work.

The requirements of Open Science are understood and incorporated into the existing environment and work model in areas like planning, risk assessment, and mitigation. This work is done in coordination with Open Science Grid.

In FY2008, two external assessments of central services were completed. The first concentrated rather narrowly on the current state of the Computing Division's Help Desk and made [recommendations](#) to align the Help Desk with the Service Desk components of the Information Technology Infrastructure Library (ITIL) framework, an internationally recognized and accepted framework for IT service management (ITSM). The second assessment looked more deeply at IT services across the Laboratory and made recommendations for a roadmap leading to ISO20000 certification on a two year time scale (FY2011), and organizational changes consolidating the "silos" of IT support across

the Laboratory. These assessments, and in particular the ISO20000 certification roadmap, form a major part of the strategy for central services for the next two years.

Vision

Be the provider of innovative, high-quality, secure common computing services. By providing these common services, contribute to the Laboratory's successful execution of the current scientific program, while positioning the Laboratory to successfully compete for future scientific projects.

Stakeholders

Sponsors: Computing Division management; Laboratory management; DOE management;

Customers: All users of Fermilab computing resources, world-wide, regardless of affiliation;

Providers:

Goals and Objectives

Overarching Goals

- Achieve “operational excellence” by following best practices for service delivery, quality and change control, customer service and satisfaction, etc., through implementation of the ITIL framework leading to ISO20000 certification by 2011. This is a transformational cultural change which will have significant impacts on all aspects of delivery of central services.
- Fully centralized management of IT infrastructure and services at the lab, encompassing all of the currently disjoint and private IT, telephony and cyber security infrastructure of AD and Business Services and other areas of the lab (a Computing Division strategic goal).
- Stable and secure operating environment which is flexible and responsiveness to user needs.
- Services “marketed” and used throughout the Laboratory (scientific & business applications).
- Plans developed one year ahead and resources in place at least 6 months ahead of need.

Central Services

- Provide robust, stable and secure production central IT services, including email, web, printing, global file services, etc.;
 - Increase the level of support and the level of security for all centrally-provided services;

- Provide robust, stable and secure infrastructure to support the major operating systems, e.g. sw distribution, patching, inventory & config control, licensing, etc.
- Provide innovative new services which anticipate customer demand;

Customer Services

- Increase customer support staff and end-user effectiveness through training and documentation.
- Improve end-user experience through more intuitive and user-friendly interface for customer support.
- Better automation and integration of account processing.
- Position to be support centers for OSG, LHC, ILC, etc.
- Provide support for major desktop operating systems – Windows, Linux, MacOS.
- Collaborate and integrate efforts across the whole Laboratory, including cross-pollinating best practices. Successfully market services to other Div/Sec.

Scientific Applications & Databases

- Support running experiments at appropriate levels and be ready for LHC and ILC requirements.
 - Agile response to new and rapid shifts of responsibilities and demands accompanying the end of Run II data taking and loss of effort in the Run II experiments;
- Develop stronger expertise and support for open source databases and tools, reducing the dependency on Oracle, with a goal of reducing development and support costs.

Infrastructure Applications & Databases

- Lead the way in providing modern information management systems that help efficiently manage the work of the Division and the Laboratory, provide information on resources and performance at all levels, and lead to easier communication.
- Develop and support those applications which are needed to improve the efficiency of the Division while avoiding duplication of functionality provided by other parts of the Laboratory.
- Apply focused effort to improving the efficiency of the HelpDesk in processing accounts and node registration, specifically.
- Successfully market new applications to other Div/Sec to further reduce redundant effort and improve efficiency.

Computer Security

- Decrease the response time to threats by automating processes currently done by humans;
- Deliver security related services in a way which solicits the willing support of users;
 - Deliver services which are palatable to end-users.

- Encourage a participatory culture & integrated security management which gets people “on board”.
- Remain proactive in understanding and guarding against new threats while maintaining an appropriately open computing environment.
- Maintain our security life cycle process – documentation, certifications, process, auditability, etc. – at levels which comfortably assure our ability to operate.
- Continuously improve computer security training programs to maintain user and sysadmin skills and respond to new threats and technologies.

Strategies

- “Sell” management support of the high-level goal to centralize management of IT infrastructure and services at the Laboratory. Achieving this goal will require a set of business management strategies which demonstrate the cost-effectiveness and other benefits to the Laboratory.
- Apply formal ITIL-derived best practices to the delivery and support of services. The ITIL framework applies across the whole range of activities and implements a number of key processes, among them continuous service improvement.
- Demonstrate the effectiveness of these first two strategies by achieving ISO20000 certification by 2011.
- Vigorously encourage use of central services; This means central services have to be useful, easy to use, flexible, responsive, performant, etc., and aggressively marketed to the end-users.
- Continue to encourage the involvement of the user community in the decision process, through e.g. Windows Policy, Unix Users, GCSC meeting, sysadmin meeting, web users group, database users group, network policy group, etc.
- Increase efficiency and integration across the Laboratory, collaborating better with other Div/Sec/Exp’s on common projects, and by aggressively looking for opportunities to reduce redundancies and consolidate efforts.
- Reduce effort and increase efficiency through effective collaboration with other labs and institutions (particularly taking advantage of FRA relationships with ANL and UC).
- Outsource or use consultants where appropriate, to fill gaps in effort or expertise. This includes considering outsourcing major efforts where cost/benefit analysis supports the decision.
- Think long-range for enterprise solutions – not “labware”, use supported (commercial or open source) solutions, pay attention to TCO in build-vs-buy decisions.
- Use common methodologies, tools and frameworks for application development to achieve consistency and efficiency. Applications should share common support data and methods (not duplicate them).
- Use automation wherever practical and cost-effective.
- Investigate and adopt rigorous development and test methodologies which provide rapid turnaround for projects without sacrificing production quality.

- Maintain life cycle processes which anticipate user needs, changes in technology, growth (or decline) in demand, etc. and allow for tactical plans to be developed twelve to eighteen months ahead, with implementation six months ahead of need.

Resource Needs

Staffing for central services will necessarily remain approximately static. Expertise in several critical areas – web services, email, shared storage, backup, for example – is very thin with perhaps one real “expert” with little backup and limited prospects for developing other staff as backup. In addition there is the need to free enough effort to continue to evolve current services and investigate new ones.

The transformation of our IT processes into the ITIL framework will require additional resources (effort) in the short term, before beginning to produce larger long term gains as more efficient processes are established and IT services are consolidated across the Laboratory. Consolidation will make some of these resources available in the short term, but we will have to rely on use of consultants for much of this effort.

Limited staff resources will increase the need for effective collaboration and aggressive consolidation of efforts across the Laboratory, as well as for use of contractors or consultants and outsourcing. The alternative is to reduce levels of service and slow (or halt) the introduction of new services, which will have an adverse effect on the Laboratory’s ability to support the current and future program.

Progress Indicators

Indicators of effective progress include:

- Progress towards service excellence indicators derived directly from the ITIL framework;
- Use of central services by a substantial portion of the Laboratory’s scientific and business program, as measured by the number of organizations and users supported, rather than equivalent local solutions;
- Improvement of the levels of central services, as measured through SLA and MOU agreements and actual service delivery, and through internal, peer and external reviews, etc;
- Maintaining high “scores” for internal, peer and external reviews of computer security process and documentation, combined with acceptable low actual rates of vulnerabilities, incidents and similar technical indicators.

Additional Information

