

**Application for
The Northwest Academic Computing Consortium
Joanne R. Hugj Excellence Award**

Risk-Based IT Change Management

**Pacific Northwest National Laboratory
IT Services Division**

Abstract:

In organizations without a formal information technology (IT) change management process, it is estimated that 80% of IT service outage problems are caused by updates and alterations to systems, applications, and infrastructure. Consequently, one of the first areas to address to improve service reliability is to track all changes and systematically manage change with full knowledge of the risks of the change and the potential organizational impact. While tracking change events is fairly well understood and is a common practice, consistently and reliably predicting the impact of change requires a disciplined, standards-based approach to assessing risk and likelihood of impact, a technique not usually found in off-the-shelf change tracking tools.

The Pacific Northwest National Laboratory (PNNL) has deployed a method and software tool to assess and track the impact of infrastructure and application changes as part of a formal release management process. The approach evolved from the experience gained from years of formal change management, as well as the influence of standards and the inspiration of service management process benchmarks such as ITIL. Unique to PNNL's process is a graded approach to change control based on intuitive assessments of risk and impact.

Description of the Practice:

PNNL IT Change Management Process Overview

Change Management is an essential part of the overall process to ensure the reliable delivery of information technology services. The PNNL infrastructure consists of over 2,400 highly interdependent applications, devices, and service functions (excluding thousands more user workstations and research project-specific devices and applications). The complexity of the infrastructure increases the difficulty of providing reliable services; change management becomes the pivotal element to manage these resources effectively.

PNNL's approach to managing infrastructure changes focuses on controlling the integrity of information systems and resources, including all network devices, computer systems, applications, and databases in the infrastructure. To accomplish this, the change management process tracks all changes and requires reviews and approvals commensurate with the potential impact of the change. To promote thorough consideration of change impact prior to instituting the change, the process is integrated with the PNNL systems and software development lifecycle: change risks are considered before systems are built and tested (Figure 1). Modifications to the change release plan during the build and test phases are allowed, but the plan will be reviewed before implementation is approved. After implementation, a release status report records the success of the change, permitting self-assessment of change effectiveness.

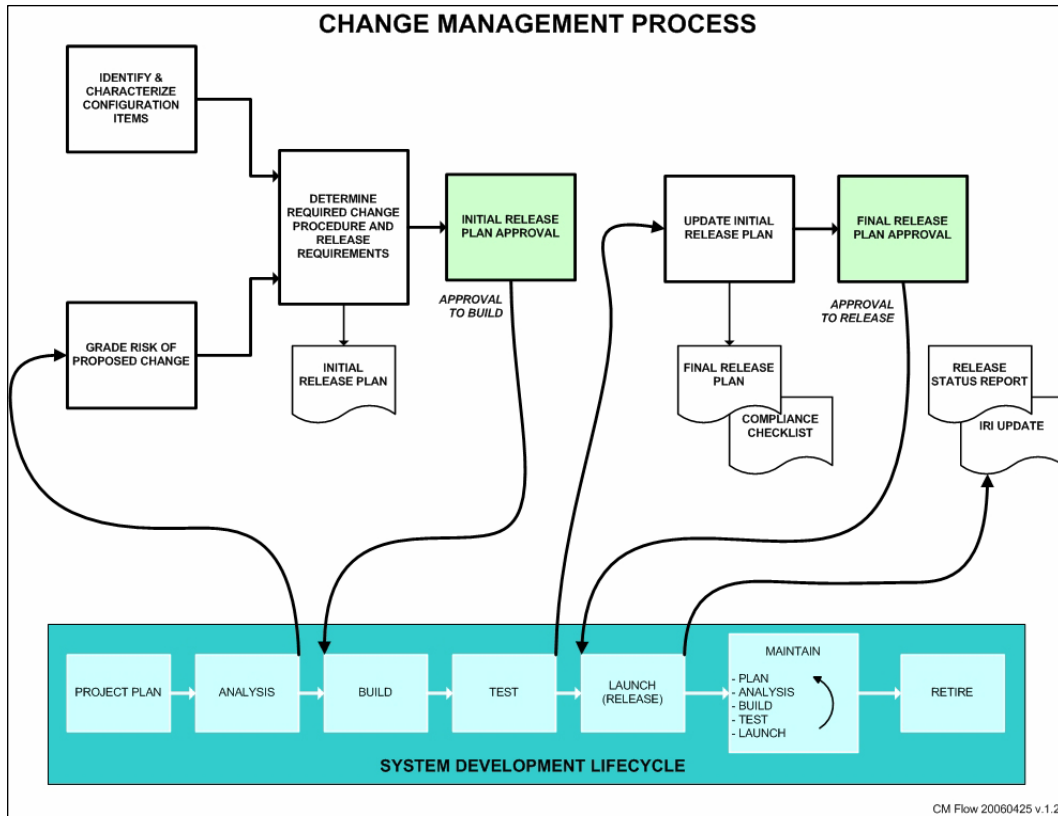


Figure 1. Integration of change management into PNNL's system development lifecycle process.

Looking at System Criticality and Change Risks

PNNL's approach differs from many formal IT change approval and tracking methods because it utilizes a standards-based approach to determine and address the risks of changes. Joined with an evaluation of the changed system's criticality to the overall enterprise, the resultant composite risk assessment prescribes mitigation requirements and strategies to be used when the change is implemented. By consistently evaluating system criticality and change risk, the Laboratory is assured of more reliable IT services since all known issues dealing with risk mitigation will be addressed with each proposed change. The process tracks the risk assessments, records change request approvals, and captures change implementation lessons-learned information that is used to influence reduce the impact of future changes.

The automated process for determining composite risk assessment is broken into two standardized evaluations: the organizational criticality of the system to be changed and the likelihood of adverse impact resulting from the change. First, on an annual basis, the criticality of the system is appraised in order to establish its relative value to the enterprise. The standardized criteria for this assessment are:

- Number of users that could be impacted by a service interruption
- Financial impact of an extended service outage or unrecoverable loss of data
- Likelihood that a system/service failure could result in:
 - Disclosure of sensitive information that needs to be protected
 - Misuse of client-owned resources
 - Malicious interruption of services or research operations

- Possibility that a system/service failure could result in an event or condition that may have adverse safety, health, security, operational, environmental, or mission implication
- Potential future impacts based on prior system/service interruption experiences

Secondly, when a change is proposed, each request is graded against the following criteria:

- How many users will be visibly affected by the proposed change?
- What is the anticipated difficulty for user and support personnel to learn the new or modified system/service?
- What is the stability and supportability of the technology or vendor products utilized by the system?
- In the event the change implementation fails or adversely impacts other systems or services, what will be the impact of executing the implementation contingency plan?
- Based upon past experience, what is the likelihood of failure or adverse problems resulting from the change?

The criticality appraisal blends with the change risk evaluation to produce a composite risk assessment that is used to pre-populate an automated release plan that guides the implementation of the change (Figure 2). Depending on the level of the composite risk, requirements of the release plan such as testing rigor and end-user communications are strengthened to mitigate higher levels of risk. Conversely, a lower risk score results in a reduced scope of change implementation requirements.

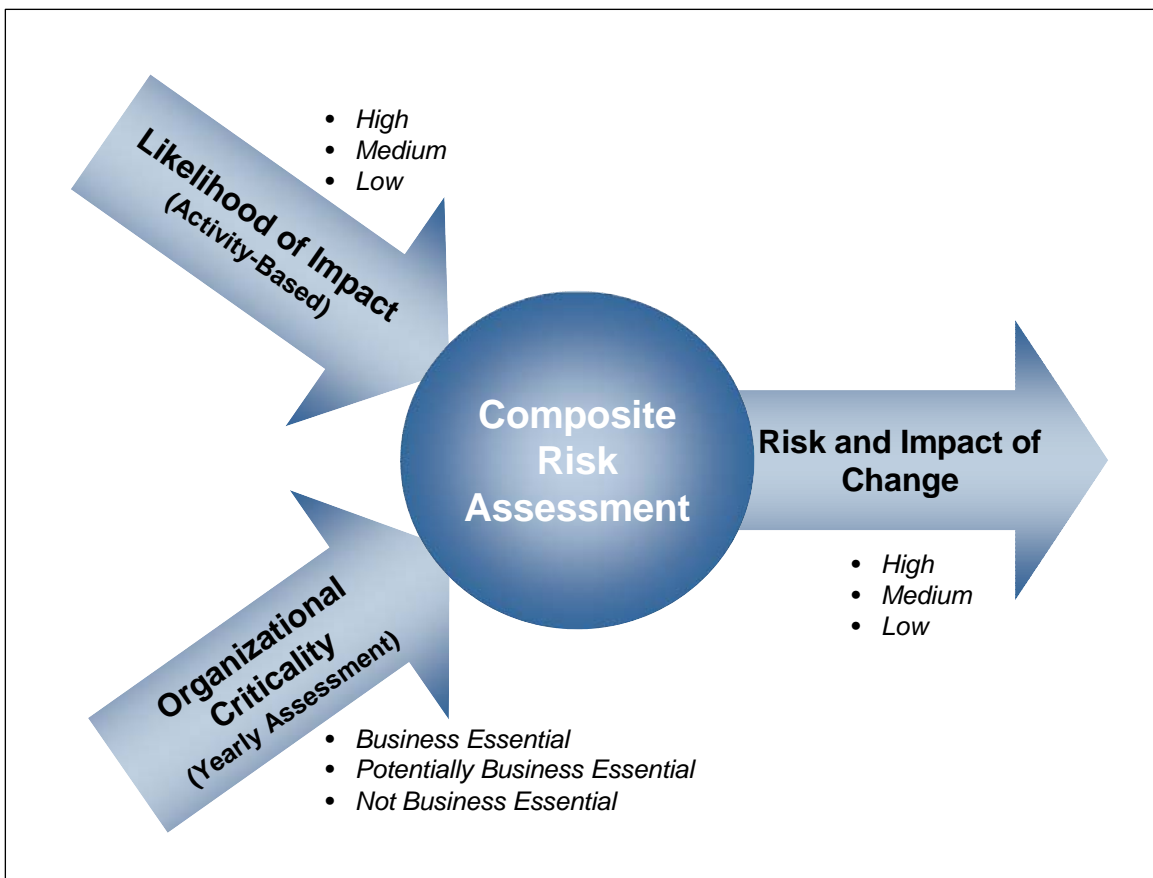


Figure 2. Combining organizational criticality and change risks.

Automating the Process

The change request and change risk assessment process is conducted through an automated system that tracks and records reviews and approvals.

The keystone to the automated system is PNNL's Information Resource Inventory (IRI), a custom built, web-based configuration management database. PNNL had invested in the IRI well before automating our change management process. The IRI was seen as a keystone not only to this process, but others such as establishing and managing service level agreements, resource and application cost reporting, cyber security compliance tracking, property administration, business continuity, and customer relationship management. To support change management, the IRI contains system criticality information as well as owner, operational contact, and service function information. In the future, the central configuration management database will provide system interdependency information critical to determining change impact of the Laboratory's highly interconnected systems and services.

The change request form (Figure 3) is used to assess risk of the change through a consistent and objective set of questions, and to document the release plan, covering topics such as communications, training needs, ongoing operational support requirements, and release contingency plans. The form was implemented using Microsoft InfoPath. Change forms are stored and managed in a Microsoft SharePoint-based document repository. Using these tools, PNNL developers were able to deploy the new system in 12 person-weeks, and have been able to easily and quickly modify the forms as we've evolved our process through experience.

Process Success Factors

The PNNL change management practice combines the composite risk assessment method with an automated process for proposing the change, obtaining approval, and recording post-implementation lessons learned. The overall process met critical success factors for the deployment of changes into the organization's crucial IT infrastructure. The success factors were:

- Implementing changes is a repeatable process.
- Changes are made quickly and accurately, driven by business needs.
- Services are protected when changes are made to optimize risk exposure.
- Utilizing the process delivers efficiency and effectiveness benefits.

By prescribing a consistent approach to evaluate change risk, the overall change review cycle is shortened. Prior to this method, 35% to 50% of all proposed changes required Change Management Board (CMB) approval, a face-to-face presentation and discussion where the change proposal author was subjected to questions from infrastructure leadership and system owners concerned about change impact. In this forum, the questions were seldom consistent; occasionally key issues were not effectively addressed as a result. The risk-based process now provides the missing consistency and allows many change requests to be reviewed and approved outside of the traditional, once-a-week CMB meeting. The number of proposals requiring full board review and approval has dropped to 6.5% of all proposed changes, improving approval cycle time accordingly. Many change requests that used to require the author to wait a week for the next CMB meeting are now approved the same day as the submittal.

Additionally, the risk-based change process is moving the overall IT organization's service delivery maturity from reactive actions to those that are well defined and repeatable (Figure 4). The standardized approach to assessing risk and tracking change release assures repeatability. Self-assessment after change completion will assist the organization to more accurately predict change risk and impact, eventually leading to managing the risk of change when systems are built, rather than after they are deployed.

Form1 - Microsoft Office InfoPath 2003

File Edit View Insert Format Tools Table Help

Type a question for help

Change Request Form

CMB Tracking Number (Assigned when form is Created):
07-1114371530

Change Type: Select Type Of Change

Description: Replace report query module to enhance user interface. Change will be made to web page content code only, not to any databases or other information.

System/Service Information *Information provided by the IRI*

Name: Information Resource Inventory (Software)

Description: The Information Resource Inventory (IRI), version 2.1, is an application used to track the Hardware and Software managed by the Information Resource Management System (IRMS). Organized into hierarchies, the system captures the relationships between the various components giving IRMS staff a tool for planning or reacting to events as required.

Type: Software

Status: Active

Owner: Johnson, Gerald R

Portfolio: Information Resource Management

Criticality (Must be updated annually in the IRI)
(High=Business Essential, Moderate=Potentially Business Essential, Low=Not Business Essential)

Level: Potentially Business Essential

Date: Nov 9 2005

Change Risk Assessment (Grade Risk of Change)

The following assessment must be completed for **every** proposed addition or modification to the system/service.

How many users will be visibly affected by the proposed change?
a) The change is transparent, or an individual or small workgroup is affected

What is the anticipated difficulty for user and/or support personnel to learn the new or modified system/service?
a) The change is transparent or intuitive

What is the stability and supportability of the technology and/or vendor products used?
a) Stable technology and vendor products; broad knowledge base and support

In the event the change fails or adversely impacts other systems or services, what will be the impact of executing the contingency plan?
a) Negligible service outage and no loss of data

Project/product manager assessment of the likelihood of failure or adverse problems resulting from the proposed change.
a) Unlikely

Change Management Category:

Category A

Criticality Level (IRI)

		Potentially Business Essential		
		Not Business Essential	Potentially Business Essential	Business Essential
Change Risk Level	Low	A	A	B
	Mod	A	B	C
	High	B	C	C

Figure 3. The Change Request form.

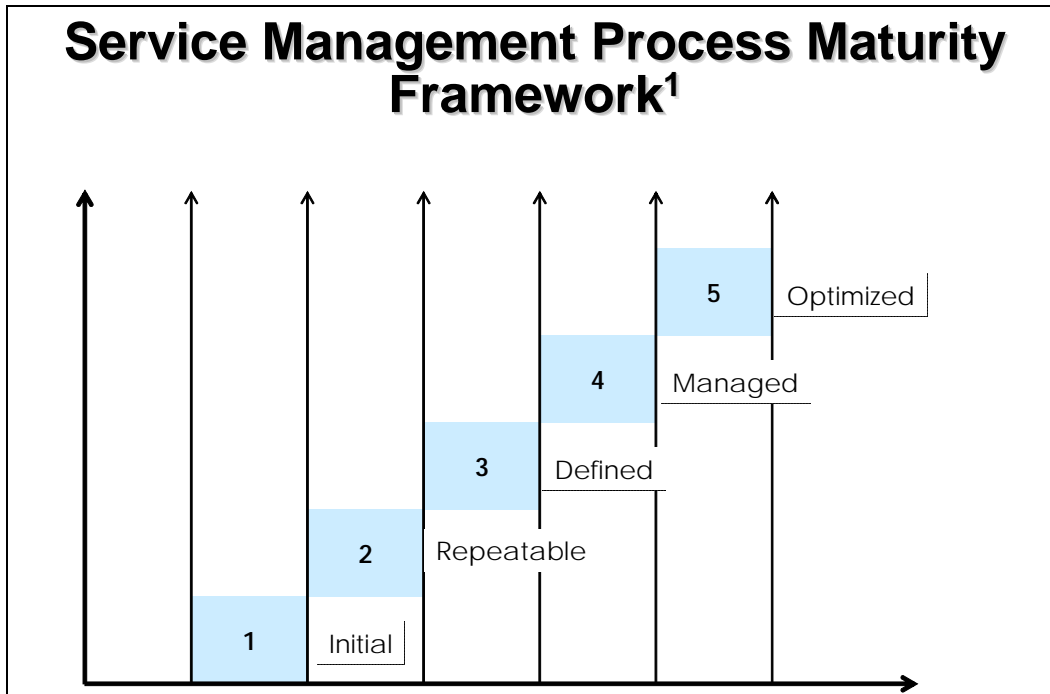


Figure 4. The Service Management Process Maturity Framework is a useful tool for evaluating IT service delivery method development effectiveness and for benchmarking against industry best practices. (¹Office of Government Commerce, ITIL Best Practice for Planning to Implement Service Management, p. 44.)

Responses to Evaluation Criteria:

Innovation

- The change approval and tracking methods utilize a standards-based approach to determine and address the risks of changes.
- The change risk assessment is tightly integrated with the central configuration management database that assesses, records, and applies the system's organizational value to the determination of risk and resultant release plan.

Benefits

- The Laboratory is now assured of more reliable IT services because system criticality and change risk assessments are standardized, encompass known issues, and evolve as experience matures.
- Change implementation impacts are known before systems are built and tested because the change management process is integrated with a standard systems and software development lifecycle.
- The overall change review cycle has shortened significantly since there is a high level of confidence that change impact issues are properly and consistently evaluated. Committee review and approval of change requests dropped by more than a factor of five. Most requests are now approved the same day rather than collecting and reviewing weekly.
- Overall service delivery improved and is better defined and more repeatable. Self-assessment after change completion contributed to evolution of the change risk assessment as well as improvements to the overall change management process.

Replicability

- This process is applicable to any organization managing change of its IT infrastructure devices, systems, and services. A versatile, central configuration management database is an essential element of this process, used for measuring and recording overall risk and impact to the enterprise.

Costs

- Process administrative costs remain approximately the same, but higher reliability and shorter approval cycle times has benefited Laboratory productivity.

Links:

None.

Principle Contact:

Jan E. Goolsbey
Jan.Goolsbey@pnl.gov
(509) 375-2018

Other Key Contributors:

Frank Carr
Frank.Carr@pnl.gov
(509) 375-2119

Wendy D. VanArsdale
Wendy.VanArsdale@pnl.gov
(509) 375-6419
