

**PATCH MANAGEMENT:  
CHANGE, CONFIGURATION AND RELEASE  
OR SOMETHING MORE?**

**By Grant Adams  
Principal Consultant  
Fox IT**

**March 2007**

## PATCH MANAGEMENT

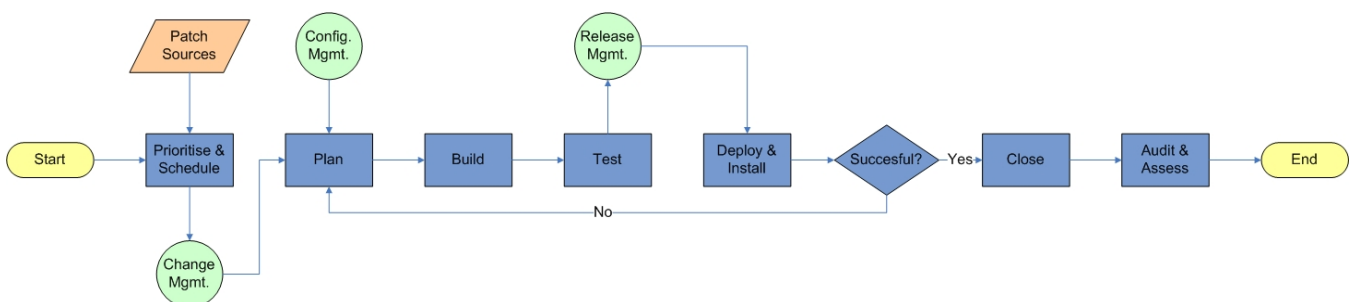
Ask many IT Managers what Patch Management is about and they'll respond that it is mostly the deployment of Service Packs and patches required to keep worms and viruses at bay. As IT infrastructure becomes more complex and businesses demand reduced downtime; coupled with the increasing anxiety around governance and regulatory compliance, e.g. Sarbanes-Oxley and HIPAA; IT Managers are required to gain greater and sustained control of their IT assets. To ensure these challenges can be met, IT Managers are increasingly endeavouring to ensure that the configuration of their infrastructure is consistent and secure. This is not limited to server operating systems and applications, but includes enterprise business applications; remote workers; desktop operating systems and office applications. With the rapid development of these and the decreasing "time to exploit" of recent worms and viruses, IT Managers are under mounting pressure to safeguard the confidentiality, integrity and availability of their infrastructures. This has ensured that Patch Management has a greater priority than ever before.

Patch Management, like any other IT service, requires people, process and technology. The marketplace contains a plethora of automated software tools to manage and control patch deployments; but how can we ensure that these tools are executed appropriately by skilled, technical staff? Robust, dependable and repeatable processes, that's how!

## PATCH MANAGEMENT PROCESS DEVELOPMENT

Many IT Managers have looked to best practice frameworks, such as ITIL and MOF to provide guidance in the development and execution of their Patch Management processes. Numerous organisations base their patch management process exclusively on change, configuration and release management. The benefit of this approach will help to ensure that the patch is deployed using standardised methods in order that the impact of any patch related incidents are minimised, and will also ensure that the IT infrastructure affected can be identified, controlled, maintained and verified whilst all aspects of the patch both technical and non-technical, are considered together. Whilst all of this is helpful, it still leaves many vital questions unanswered.

## TYPICAL PATCH MANAGEMENT PROCESS



We may have implemented what, at first glance, appears to be an efficient process, but how do we identify what the unanswered questions are; why are they important and how do we answer them?

To determine what those unanswered questions are, we need to examine the Patch Management strategy. If the strategy deals only with controlling patch deployments, then it is likely that there are few unanswered questions. But consider this; would the business and its stakeholders be satisfied with a well deployed patch that created service vulnerabilities? Absolutely not. Protecting the current environments is of equal importance to successfully deploying patches. This suggests that the scope of the strategy need to be broadened to include the protection of the existing test and production environments.

Whilst it is generally accepted that any new software update, including patches need to be assessed; identified; evaluated and planned; and deployed, how can we ensure that all aspects of the service, technical and non-technical, that the patch supports are considered? How do we identify the required patches? What criteria are patches assessed against and how are they prioritised? What standards exist to manage the building, testing and implementing of patches? How will patches be decomposed prior to re-building? Where will they be tested? How will they be deployed and installed? Where will the configured patch be stored and how will it be stored? How will we assess the business impact? How will we recover from unsuccessful patches? How are standard builds updated to include deployed patches?

All of these questions and many more can be identified and answered by mapping an organisation's Patch Management process to ITIL.

|   |                          |
|---|--------------------------|
| Is the patch assessed for suitability, function and purpose?                                      | <input type="checkbox"/> |
| Are configuration details recorded?   | <input type="checkbox"/> |
| Is there a separate Test and Production environment?  | <input type="checkbox"/> |
| Is a record or inventory kept of the Production and Test environment's components?                | <input type="checkbox"/> |
| Is there an established testing area and methodology?   | <input type="checkbox"/> |
| Is there an established risk assessment and contingency planning methodology?                     | <input type="checkbox"/> |
| How does identification of the need for an update occur?  | <input type="checkbox"/> |
| Is the update relevant to this environment?   | <input type="checkbox"/> |
| Are all the details of the update available, e.g. in bulletins or reports?                        | <input type="checkbox"/> |
| Can a preferred implementation time be identified?  | <input type="checkbox"/> |
| Can the patch be obtained from source and verified as safe, secure and free from virus infection? | <input type="checkbox"/> |
| Is a recognised Project methodology to be used?   | <input type="checkbox"/> |
| Are there dependencies to be planned for and managed, e.g. size, capacity constraints?            | <input type="checkbox"/> |
| Has the deployment method been identified, agreed and planned for?                                | <input type="checkbox"/> |
| Is there a formal process for accepting new Releases or Updates into Deployment?                  | <input type="checkbox"/> |
| Is there a mechanism for monitoring and controlling the deployment?                               | <input type="checkbox"/> |
| Is there a mechanism for dealing with stalled or failed deployments?                              | <input type="checkbox"/> |
| Is a new Baseline for the updated environment required?   | <input type="checkbox"/> |

# MAPPING PATCH MANAGEMENT TO ITIL

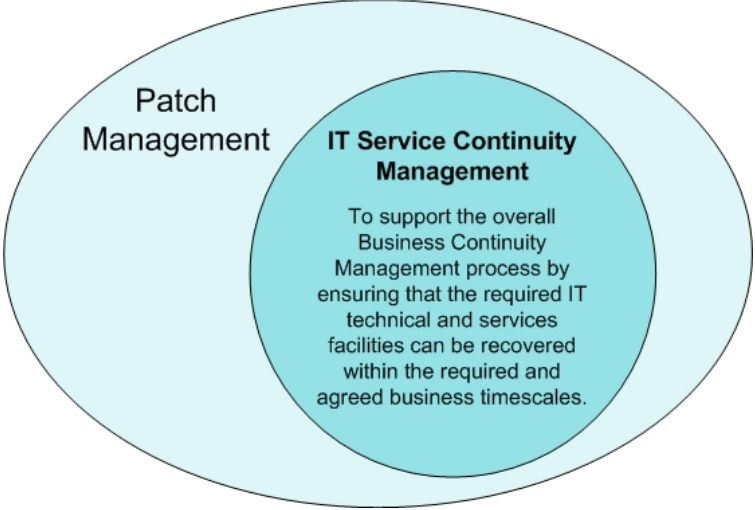
Mapping an organisation's patch management requirements to best practice service management will ensure that all aspects of service management are considered in the development of the patch management process.

Through this sort of mapping exercise it is possible to identify the activities that ensure that the patch is deployed properly **and** the production environment is protected.



## ENHANCED PATCH MANAGEMENT PROCESS DEVELOPMENT

To assist in the identification of the questions that you need to answer, consider the objectives of the service management processes against the backdrop of patch management. For example;

| <b>IT Service Continuity Management</b>   |   |
|---|---|
| <p>How will we fulfil our mandatory and/or regulatory requirements in the event of a service failure caused by a failed patch deployment?</p> <p>How will we manage business disruption during an incident caused by a failed patch deployment?</p> <p>In the event of service outage as a result of a failed patch deployment, how will we recover services efficiently in business priority order?</p> <p>Have we updated our Continuity plans to reflect recent patch deployments?</p> |  |

It is only when you have considered all of these issues that you can begin to develop an enhanced patch management service that will ensure that your patches are deployed successfully whilst also protecting your test and production environments.

## **ABOUT FOX IT**

Fox IT is a global IT Service Management and Governance company, providing organisations with consultancy and education in methodologies and technologies that help them to align their IT operations with their business strategy to ensure good IT Governance.

Fox IT provides Patch Management services that are designed to ensure that an organisation has efficient Patch Management processes and has effective operations staff who understand their responsibilities and are able to achieve maximum benefit from the appropriate tools and technologies.

Fox IT can be contacted by telephone on +44 (0) 1483 221200 or by email to [sales@foxit.net](mailto:sales@foxit.net).

## **ABOUT THE AUTHOR**

Grant Adams is an experienced Service Management professional with over 16 years experience of technical, service, project and line management duties. Grant has qualifications in ITIL, MOF, ISO20000, Prince2 as well as many technical qualifications relating to the Microsoft environment.

His experience includes many years in the planning, building, deploying and operating of medium to large Microsoft infrastructures. This has resulted in Grant being Fox IT's lead consultant in the delivery of IT Service Management in Microsoft Environments. He has developed and delivered service management consultancy services for the assessment and implementation of Patch Management; Managing Active Directory and Group Policy Objects; and Developing and Deploying Server Build Images using MS ADS. He is currently leading the development of consultancy and training services focused on Microsoft's Infrastructure Optimisation Initiative and Dynamic Systems Initiative.

In addition Grant has worked with other technology suppliers to develop supporting processes such as Storage Management for Hitachi Data Systems.

Grant was involved in the development of Fox IT's ISO20000 Service Line and brings practical experience of assisting a major UK banking organisation to achieve ISO20000 certification.

Grant is also accredited by both the ISEB and EXIN to deliver service management training courses and is a Member of the British Computer Society.