OOMC
Patch Management
Guide

OPTION ONE
MORTGAGE

Contents

Chapter 1

Overview

This document is the definitive guide to be used by all teams involved with OOMC patch management and deployment. The term *patch management* describes the tools, utilities, and processes for keeping computers up to date with new software updates that are developed after a software product is released. *Security patch management* is a term used to describe patch management with a focus on reducing security vulnerabilities.

Patch management life cycle is described as the process of controlling the deployment and maintenance of interim software releases into production environments. It helps maintain operational efficiency and effectiveness, overcome security vulnerabilities, and maintain the stability of OOMC production environment.

This guide discusses a streamlined process for security patch management. It also defines key issues, concepts, and best practices related to patch management.

Patch Management Committee

Proactive security patch management is a requirement for keeping OOMC's environment secure and reliable. As part of maintaining a secure environment, a Patch Management Committee was developed. The Patch Management Committee will be referred to as the Committee throughout this document. The Committee is represented by individuals from various IT Teams. The goal of the Committee is to develop a patch management program that includes vulnerability awareness, process and procedures for timely mitigation of risks. The Committee ensures patch management is carried out effectively, as part of normal operations. The Committee also applies software updates, makes configuration changes, and tests the applied changes. The progressive methodologies provide countermeasures to eliminate vulnerabilities from the OOMC environment and mitigate the potential risk of computers being attacked.

The purpose of this Guide is to present an introduction to OOMC's Patch Management initiative. It serves to educate everyone on the processes, roles and responsibilities of the Committee, and the impact on critical business processes from proactive patch management. Ultimately, this guide will be the foundation of a successful patch management program. Changes to the Guide shall be based on the approval of the Committee. The Guide shall be updated on an as need basis.

Finally, successful patch management, like security operations, is achieved through a combination of people, process, and technology.

Patch Management Etiquette

The members of the Patch Management Committee are expected to abide by the rules set forth in the Guide. Successful patch management relies on active participation of all members of the Committee. This section discusses the etiquette and expectations of the members within the Committee.

> **Important Note:** The bi-weekly meetings are **mandatory**.

Schedule Meetings

There are three types of meetings:

Meeting type	Held When?	Purpose
Bi-weekly Patch Meeting	2nd Wednesday and 4th Wednesday. Or, as needed for emergency or same day as released Microsoft security Bulletin. 2:00 PM to 3:00 PM	▪ Identify risks association with new vulnerabilities. ▪ Review new security vulnerabilities ▪ Determine plan of action, specific dates for test and deployment of patches ▪ Assign and Review action items as necessary ▪ Confirm teams understanding and acknowledgement of meeting discussion.
Pre-deployment Patch Meeting	The afternoon before any deployment in production environment. 3:30 PM to 4:00 PM	▪ Confirm list of servers/applications ▪ Review task lists of each team ▪ Confirm resources availability ▪ Confirm and finalize all changes
Post-deployment or Lessons Learned Patch Meeting	The day after a deployment is production environment.	Purpose is to discuss: ▪ What as done right ▪ What needs improvement ▪ Completion percentage servers, desktops and exclusions scheduled for next deployment.

Meeting Attendance

Meeting attendance is mandatory-no exceptions. Bi-weekly meetings are crucial to the development, definition, and communication of patch details, rollout timelines, and resources. It is the responsibility of each team to ensure that a representative attends the meetings. Refer to Meeting Minutes if your team is unable to attend the meeting. Your Team Lead or Manager is responsible for completing any assigned tasks to the respective member. Your absence from the meetings will waive all rights to any decisions made during the meeting by the meeting attendees. These decisions may include:

- The dates of patch deployments to DEV, TEST, Staging/QA and Production

- Which Security Patch(es) to deploy

- Which list of servers or applications to deploy the patch

- Assigned tasks to specific member

- Resource allocation

- Any new development or changes pertaining to the Patch Management guidelines set forth

Therefore, any determination of security patches, patch dates, and/or server or application lists cannot be changed without the written business justification and explicit approval from the Patch Coordinator, Brian Bargy and Change Control Board (CCB).

Written justification to override the changes must come from a Team Lead or a Manager-level individual and include the following:

- Business justification for the change or why the patch cannot be proceeded as planned

- List of servers and application names which cannot proceed with the patch as planned

- New date for patching

The deadline for any requested changes related to production patch deployment is 11:00 AM on the day of the patch. No exceptions.

Communication

The key criterion for successful patch management is accurate and timely communication.

IT – Patch Management Distribution List

The distribution list includes the names of all members involved in Patch Management. This list is solely use to exchange information, such as announcements of patch deployment schedule, meetings, etc., among the Committee. The Distribution List can be found under the Global Address List of OOMC.
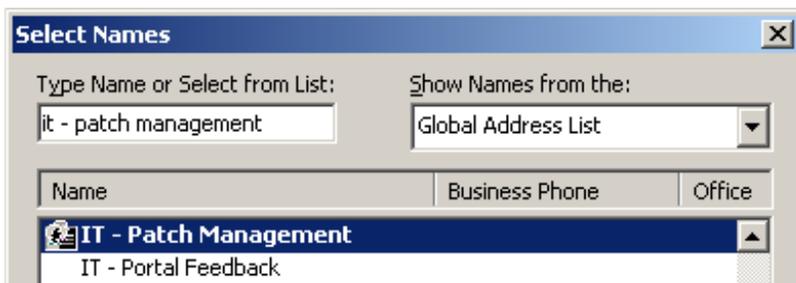
During Production Patch Deployments

All assigned resources for the evening of the patch deployment must call in the AT&T teleconference number at **9:30 PM** to check in. The teleconference will remain open for the entire duration of the patch deployment. Status updates will be communicated during the conference call. This is the required method of communication between team members during production deployments.

AT&T Teleconferencing
Number: 866-249-5352
Host ID: 426676
Time: 9:30 PM to 1:00 AM local time
Hosted by: Patch Coordinator

Sharepoint Site and IT Web Portal

All documents related to the Patch Management project can be found on Sharepoint. Eventually, the documents will be available at http://it2.oomc.com/Groups/patch_management.shtml, the IT Web Portal.

Team Responsibilities

This section provides a summary of tasks for the various team roles for all patch related activities.

Patch Management Committee

- Meets bi-monthly to discuss current vulnerabilities, plan for upcoming deployments, and continually improve the process through lessons learned reports.
- Review the details of each patch, decides whether it is applicable to the environments, determine time frame on test and implementation of patch. Assess prerequisites, sequences, and conflicts.
- Adhere to the standard procedures and guidelines that are approved and governed by the Patch Management Committee.

Information Security

- Receive patch bulletin from Microsoft and other vendor applications and software.
- Check security web sites for relevant information and establishes whether any critical patches are available.
- Evaluate patch bulletins to determine validity of patches or vulnerabilities. Identifies the source of the patch to ensure that it is from a known and trusted source.
- Prepare a summary document of the known patch or vulnerability and notify Committee of details. Ensure that the right people are notified. Sends an email announcement to Patch Management Committee for applicable or non-applicable responses.
- Determine factors that may influence patch release priority.
- Attend Change Control Board (CCB) meetings and participates in approval of changes.
- Participate in the development of security policies and standards, intelligence (monitoring the patches), as well as governance, risk assessment, vulnerability scanning and compliance monitoring.

Release Manager

- Define release policy. Provide release planning, acceptance and rollout planning. Build and review release strategy. Project manager for all authorized changes. Active communicator to all parties involved.
- Automate testing, change control, and promote to production through release management.
- Perform an end-of-day scan to establish current state of changes.
- Monitor change schedule. Monitors the changes that are due to occur and assesses any potential conflicts.
- Monitor staffing level to make sure the availability of change managers, change owners, release managers, and so on, and reassigns tasks as appropriate.
- Monitor release schedule to verify the progress of changes through Management.
- Run team meetings to plan activities for the coming week and provide a forum for good communications among all team members. Provide meeting minutes, weekly reports that outline the status of the releases—for example, in production or in rollout planning.
- Meets with business managers to discuss service levels, business requirements, and open issues. Build detailed rollout plans for a specific location or area of the business. Coordinates with the business to obtain acceptance for rollout planning.
- Report status of releases. Report on numbers of releases awaiting resources; whether the releases are open, aborted, or deployed; or whether they are in the pilot, live, or planning stage.

Compiles a report that helps identify areas of the release process that work well, others that do not, and those requiring attention.

- Review release technology to see whether more appropriate release mechanisms are available. Proactively searches for improved or more relevant technology for deploying releases.
- Schedule test resources to ensure that test resources are available for testing.
- Reviews the rollout order to take account of any scheduling constraints imposed by the business. For example, it may not be possible to deploy into the finance department on the date originally planned because of end-of-year processing.
- Review rollout preparation. Deploy release Roll back release Review escalation paths.
- Attend Change Control Board (CCB) meetings.
- Submit CAR for approval, communicate to committee on CAR ID number, and notify committee of CAR approval.
- Set up all change related meetings such as pre and post-deployment, lessons learned meetings
- Communicates all messages to committee, business units, and management of any authorized changes. This means sending out communication templates to IT Help Desk, to committee, and business units affected by the scheduled change.

Operations

- Audit development, test, staging, and production environment to get an accurate assessment of the environment before determining, or building upon operational baselines.
- Audit reports of server development, test, staging, and production environments, confirm that the audit has taken place, and compare it against previously recorded data.
- Monitor information sources for new notifications. Review patch reference files. Ensure that the latest reference files have been downloaded from the Microsoft Web site.
- Check for new patch notification locations and verify that existing ones are still valid. Download patch reference files from the Microsoft Web site. Scanning tools use these files to identify the need for patches.
- Run scanning tools such as LANDesk on workstations and ECM on servers to establish whether patches are required. Produce patch reports from each notification source. These reports should show the number of patches received, relevant, and rejected as being not relevant.
- Reviews the information and files provided with the patch to see whether there are any prerequisites, sequences, or conflicts. Review/scan reports and report to the incident management team any identified patches that have not been installed.
- Prerequisites are certain conditions must be true for the patch to install successfully. The information provided with the patch may also dictate a certain installation order (or sequence) with other patches or software applications. The material provided with the patch may also indicate that problems may be encountered if certain applications or files are present (conflicts). All details and information discovered about prerequisites, conflicts, and sequences for a patch should be recorded in the Change Management system, to assist in the decision making process and in the development of the economic and business case.
- Attend change advisory board (CAB) meetings.
- Performs the active roles of pushing out the patches to all servers

OOMC Managed Inventory

In compiling information for this guide, the Committee assessed OOMC's current inventory of software, hardware, applications, etc. Upon completion, a comprehensive document will provide and educate management and Associates of the duties and time involved to perform these vital tasks. Four key areas were discovered which are defined as follows:

Assessment

An assessment of all servers and applications in every environment provides a complete inventory of all devices attached to the network. The inventory will provide a central repository for data related to the system that can be used in evaluating potential patching strategies and processes, and then used for tracking purposes later on. The inventory should help answer questions such as those listed below:

- How many operation systems are present that will potentially need to be patched?
- How many versions of the operating system are in use?
- How many applications and application versions are in use?
- Will some OS or application versions need different patches
- How many unpatched systems are being used, and which ones are they?
- How many unmanaged systems are being used, and which ones are they?
- How many and which systems are mission critical?

Testing

The Testing environments for both servers and desktops include OOMCDEV, Testing, QA in OOMC, and Staging. After QA conducts the smoke test successfully, deployment proceeds to production.

Deployment/Rollout

Production deployments are broken up into two different nights to minimize impact of critical-mission applications. The first deployment will be applied to the Infrastructure and Oracle servers. The second deployment will be applied to all other production servers.

- Infrastructure Servers - DCs, DMZs, Exchange, Print Servers, etc.
- Critical Apps - LPS, Mortgage Flex, etc
- Auxiliary Servers - JAG Servers, etc

Maintenance

After the rollout is completed, it is important that the systems are audited to ensure the patch was applied correctly and to the appropriate systems. It is also important to confirm that the patch was not applied to systems it was not intended for. The Server Team will use ECM as the tool to scan the servers, while Desktop Applications will use LANDesk to scan desktops. Both teams will use the respective tools to compile a post-installation status report. The Committee will review how well the process worked and note any issues that came up during the rollout. Patching is an iterative process, and areas that can be improved should be identified to reduce the time and difficulty next time.

Hot Fixes, Patches, Service Packs, Updates

The Committee applies patches and fixes to maintain the security and reliability of other OOMC supported products and services. Patch management for these items include Hot Fixes, Patches, Service Packs, and Updates, not just Microsoft Security patches. Although the Microsoft patch methodology seems ideal, not all OOMC patches will be applied to the applications as defined by Microsoft.

- Operating Systems
  - Microsoft
  - Linux
- Applications
  - PeopleSoft
  - BEA WebLogic
  - JAG servers
  - Netegrity SiteMinder, IdentityMinder
- Database Servers
  - Examples: SQL, Oracle, etc…
- Third-Party Software Applications
  - Examples: FileNet, RightFax, etc…
- Network Devices
  - Examples: Cisco IOS, Cisco Routers, Switches, etc.

Patch Management – The Big Picture

As stated in the CCB, the timetable below shows how a patch progresses through the deployment cycle.

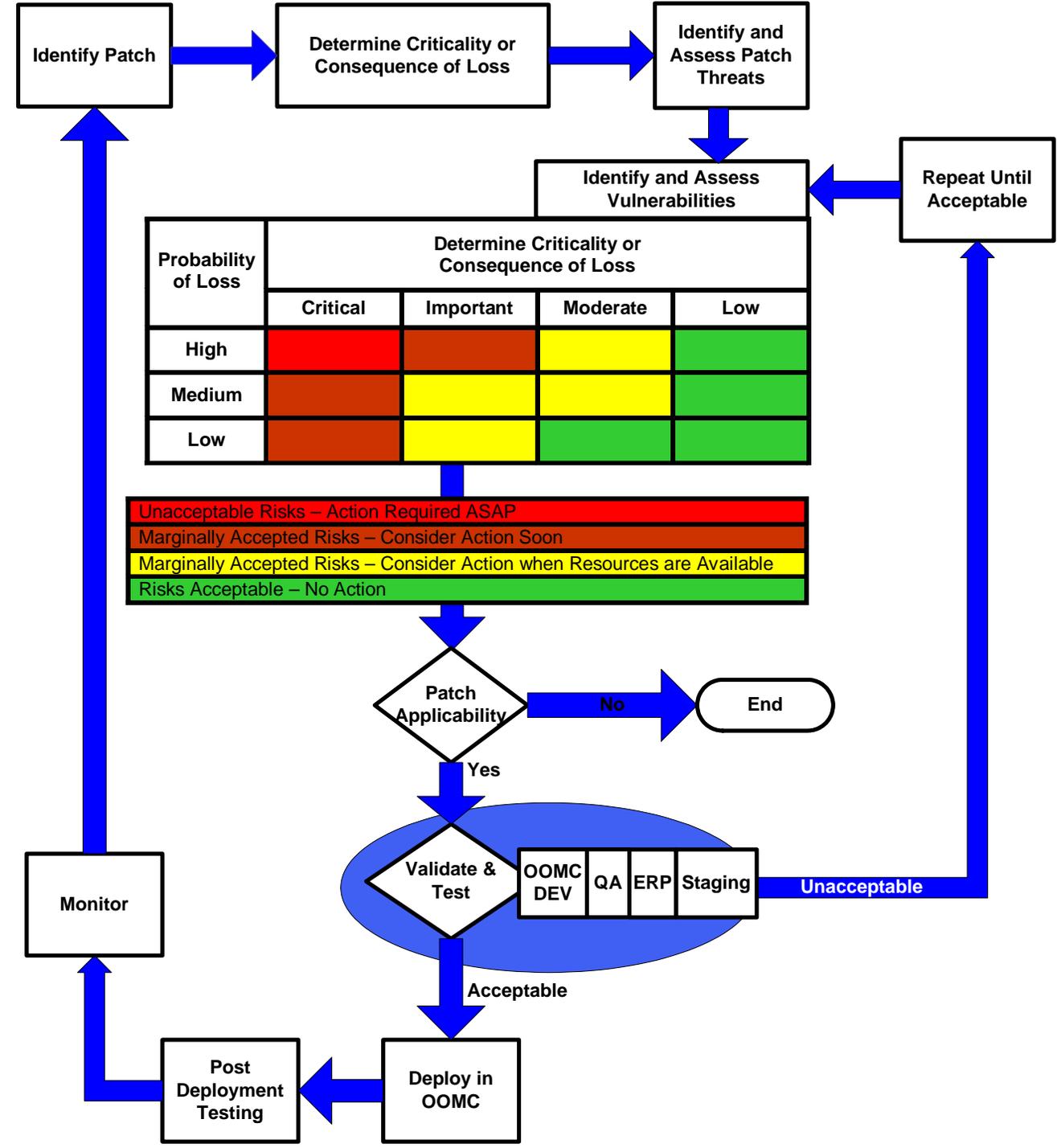| Event	Timeline	Action
Microsoft publishes security bulletin(s)	2nd Tuesday of every month	
Information Security reviews bulletin for applicability, severity, criticality	Immediately after security bulletin announcement	Information Security sends out announcement of new security bulletins to Committee
Patch Committee meeting	Bi-weekly. Usually 2nd and 4th Wednesday or as needed in emergencies will meet immediately after security bulletin announcement.	Team discusses criticality level. Define specific dates for Dev, Test, Staging, and Production.
Meeting minutes created	Maximum 2 days after meeting	Email to Committee on Thursday
CAR submitted	After decisions are made regarding timelines, which occurs during meeting	Server Team submits CAR before meeting of CCB for approval
Submission of server	Minimum 3 days prior to patch date or ASAP	Server Team submits the list of server and application names that will be included for the patch deployment
Help desk send communication to everyone affected by patch deployment	Minimum 2-days prior to deployment date	Coordinator submit communication template to Help Desk and request the memo be sent out to all recipients affected by the patch rollout
Pre-deployment Meeting	Afternoon of patch deployment	Confirm and finalize all changes. Changes acceptable only with written business justification and approval from Brian Bargy and CCB
Patch deployment task list created	Created after pre-deployment meeting	Coordinator sends out finalized task list with specific resource names for the deployment evening

Patch is deployed at 9:30 PM except for Oracle servers which begin at 7 PM.	As planned and finalized in pre-deployment meeting	All assigned resources report by calling the AT&T teleconference number
Patch deployment complete at 1:00 AM	Server Team pushes out the last patch by 12:00 AM	Coordinator: ▪ Informs Help Desk to send out communication email regarding completion status. ▪ Informs Jeff Bresnahan to close CAR ▪ Sends email to IT – Patch Management regarding status of evening
Post-deployment meeting	Brief meeting for lesson learned	All assigned resources must attend this meeting
Desktop Apps notified to deploy patch. Creates .MSI file for deployment.	2 days after rollout	
MUSTeam notified from Desktop Apps. MSI and EXE File uploaded to FTP site.		

Process Management Tables

The table below shows the Microsoft Severity Rating System. The severity rating system provides a single rating for each vulnerability.

Severity	Definition
Critical	A vulnerability whose exploitation will likely result in the compromise of the confidentiality, integrity, or availability of users' data, or of the integrity or availability of processing resources
Important	A vulnerability whose exploitation could result in compromise of the confidentiality, integrity, or availability of users' data, or of the integrity or availability of processing resources
Moderate	Exploitability is mitigated to a significant degree by factors such as default configuration, auditing, or difficulty of exploitation
Low	A vulnerability whose exploitation is extremely difficult, or whose impact is minimal

Identify Patch → Determine Criticality or Consequence of Loss → Identify and Assess Patch Threats

Identify and Assess Vulnerabilities ← Repeat Until Acceptable

Probability of Loss	Determine Criticality or Consequence of Loss			
	Critical	Important	Moderate	Low
High				
Medium				
Low				

Unacceptable Risks – Action Required ASAP
Marginally Accepted Risks – Consider Action Soon
Marginally Accepted Risks – Consider Action when Resources are Available
Risks Acceptable – No Action

Patch Applicability → No → End

Yes

Validate & Test — OOMC DEV | QA | ERP | Staging — Unacceptable

Acceptable

Monitor

Post Deployment Testing ← Deploy in OOMC

The security release deployment timeframe table provides a comparison of Microsoft's recommended timeframe to deploy a patch, depending on its severity ratings, versus OOMC's acceptable timeframe.

Severity	Microsoft Recommended Timeframe	Recommended Timeframe
Critical	Deploy within 24 hours	Deploy within one month
Important	Deploy within one month	Deploy within three months
Moderate	Depending on availability, deploy a new service pack or update rollout that includes a fix for this vulnerability within four months	Deploy the software update within six months
Low	Depending on availability, deploy a new service pack or update rollout that includes a fix for this vulnerability within one year	Deploy the software update within one year, or may choose not to deploy at all

The factors that may influence release priority table shows possible factors that may raise the level of patch priority based on its severity ratings, applicability to OOMC's environment, and other factors that might impose an even greater risk.

Environmental/Organizational	Possible Adjustment of Priority
High-value or high-exposure assets impacted	Raise
Assets historically targeted by attackers	Raise
Mitigating factors in place, such as countermeasures or patch that minimize the threat	Lower
Low value or low exposure assets impacted	Lower

Deployment Timeline

One of the goals for patch management is to ensure a consistent deployment timeline every month. With any process there are *recurring events* that aid in predictability. This predictability gives OOMC an added edge because of knowing critical operational busy times.

Significant Event	Avoid
Origination	3rd & 4th week of the month
Payroll	Anywhere from 3-5 days before payday depending on adjustments due weekends and/or holidays. See ERP team for blackout schedule. ERP will provide a new calendar at the beginning of the year.
Servicing	Middle of the month
Accounting	Month end/beginning of month

Patch Release Schedules

The Committee proposed maintenance window for all low-impact server maintenance and patch deployment for production environment has been approved by CCB. Effective January 2, 2005, the Committee shall proceed by the following timelines. *Hours of patch deployment will be from 9:30 PM to 1:00 AM local time.*

Non-Emergency

| Timeline (Monthly)	Environment	Comments
2nd Wednesday	3rd Party	Begin research with vendors for patch verification for third party applications
2nd Thursday	OOMCDEV	Deploy patch
2nd Friday	QA/TST	Pending successful result in DEV, deploys patch
3rd Friday	Staging	Pending successful result in QA, deploys patch
3rd Friday	Production	Pending successful result in QA, deploys patch to DC's, File and print servers, Exchange, and utility servers.
1st Thursday	Production	Deploy according to agreed consolidated list of apps/servers

Emergency

Timeline (Monthly)	Environment	Comments
2nd Wednesday	Development	Deploy patch
2nd Thursday	TST/Staging	Pending successful result in Dev, deploys patch
2nd Friday	Q/A	Pending successful result in QA, deploys patch
3rd Thursday	Production: Infrastructure & Oracle servers	Pending successful result in QA, deploys patch to DC's, File and print servers, Exchange, and utility servers.
3rd Thursday	Production: All other servers	Deploy according to agreed consolidated list of apps/servers

Emergency Procedures

There may be instances of security patches that require immediate action. Such is the case if an exploit is known and available on the Internet. If this is the case, the Committee will proceed with the following contingency procedures.

1. Information Security will notify the Committee of the known security bulletins or known exploits.

2. The Committee will have an Emergency Patch Meeting to determine applicability and criticality.

3. The Committee will define plan of action with timeline for test and deployment.

4. The Committee will proceed with the Emergency schedule as defined in the Guide.

5. The Committee will seek CCB for an exception to the CAR.

6. The Committee shall abide to all communication guidelines set forth in the Guide.

The Emergency deployment must be completed within one-week timeline, from evaluation, test, to deployment. The diagram below provides a high-level overview of the Emergency procedures.
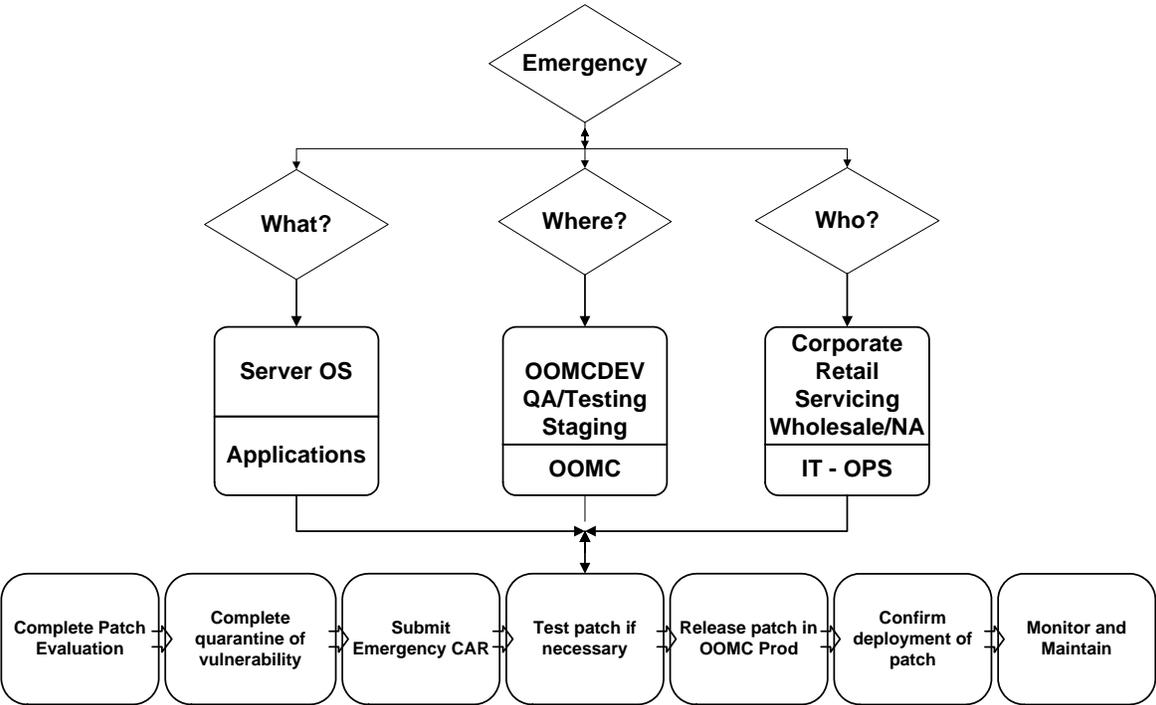
Rollback Plan

From time to time, the Committee may need to exercise the rollback plan in the event of the update not having an uninstall process or the uninstall process failing. The rollback plan can be as simple as restoring from tape, or may involve many lengthy manual procedures.

A rollback plan will allow the server and application to return to their original state, prior to the failed implementation. If something unforeseen were to go wrong because of trying to apply the patch, methods for rolling back any changes should be evaluated, documented, and tested within the reference environment before proceeding with the deployment. Patch rollbacks must be approved by the Patch Coordinator, application owners, and or the Committee. Patch roll back will be approved on a case-by-case basis.
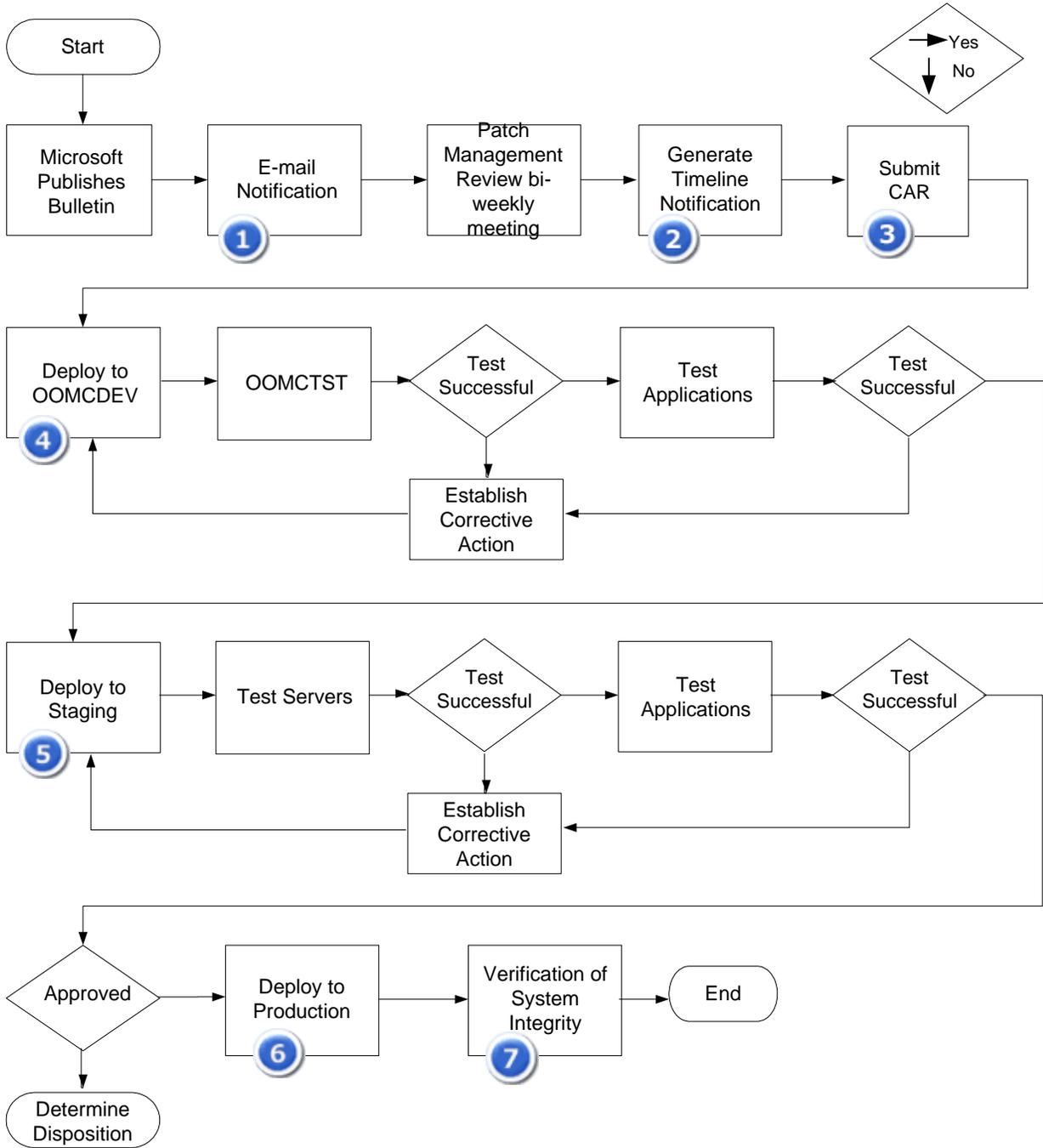
Recovery of Failed Patch

Once a patch has been roll backed (uninstalled), QA must conduct a smoke test to ensure that the application is working as it was prior to the patch. QA will document the incident and notify the Committee that their smoke test was completed successfully. In addition, the Committee must investigate why the patch failed and how it will be re-deployed again within the OOMC environment.

Patch Management Process Flow Chart

The following diagram provides a summary of the Patch Management Process that was approved and signed off by the original members of the Committee on April 21, 2004.

Start

Microsoft Publishes Bulletin → E-mail Notification **1** → Patch Management Review bi-weekly meeting → Generate Timeline Notification **2** → Submit CAR **3**

Yes
No

Deploy to OOMCDEV **4** → OOMCTST → Test Successful → Test Applications → Test Successful

Establish Corrective Action

Deploy to Staging **5** → Test Servers → Test Successful → Test Applications → Test Successful

Establish Corrective Action

Approved → Deploy to Production **6** → Verification of System Integrity **7** → End

Determine Disposition

①②	Bulletin Notification & Review	
#	**Task**	**Resource Name**
1	Sends an email announcement to Patch Management Team for Applicable or Non-applicable responses	Information Security
2	Gather email responses from Patch Management Team	
3	Determine factors that may influence patch release priority	
4	Determine patch release timeline	

③	CAR Submission	
#	**Task**	**Resource Name**
1	Patch coordinator submit CAR for approval	Server Team
2	Patch coordinator communicate to Team on CAR ID number	Server Team
3	Notify team of CAR approval	Information Security
4	Patch coordinator setup pre-deployment meeting	

④	Deployment to OOMCDEV	
#	**Task**	**Resource Name**
1	Determine affected Applications	Dev QA Server 3rd Party Middle Tier Desktop & Apps DBA ERP* (PROD)
2	Determine applicable servers based on affected Applications	
3	Communicate list of servers to Team	
4	Test Servers	
5	Test Applications	
6	Establish corrective actions, if necessary	

	Deployment to Staging	
#	Task	Resource Name
1	Determine affected Applications	Dev
2	Determine applicable servers based on affected Applications	QA Server
3	Communicate list of servers to Team	3rd Party
4	Test Servers	Middle Tier Desktop & Apps
5	Test Applications	DBA
6	Establish corrective actions, if necessary	

	Deployment to Production	
#	Task	Resource Name
1	Verification list of applications and servers to deploy patch	Dev
2	Communicate list of servers to Team	QA Server
3	Deploy patch according to established pre-deployment meeting action items	3rd Party Middle Tier
4	Test Servers	Desktop & Apps MUST
5	Test Applications	DBA
6	Take corrective actions, if necessary	ERP* (PROD)

	Verification of System Integrity	
#	Task	Resource Name
1	Server Reboot Checklist	3rd Party Middle Tier Desktop & Apps DBA
2	Verify through software inventory tool.	DESKTOP & APPS
3	Reestablish Services	QA 3rd Party Middle Tier ERP
4	Meet to discuss lessons learned, as needed	ALL

Chapter 2

Task Tables

This section shows each team and their associated tasks that are performed during patch deployment.

Note: The *Task Time* shown in the tables are an approximation and difficult to quantify due to the nature of the patch severity and complexity.

Team	**Task Time**
Call Center Technology	▪ 6 hours from manual rollout of patches to completion

Prerequisites	**Tools**
All patches that were pushed out during the past quarter will be reviewed.	▪ PC Anywhere

Dependencies

- ▪ Ensemble
- ▪ IVR
- ▪ ICM
- ▪ ECM
- ▪ WFM
- ▪ Witness

Procedures

Identify necessary patches for Contact Center Servers

Notify business with quarterly schedule for patch rollout.

Notify vendors with quarterly schedule. Align vendor support for rollout. This includes Norstan & Concerto.

Manually install patches, verify successful installation, test environment.

Communicate successful test completion to the team and business.

Resources to be onsite by 5:00 A.M., day after patches:

Dan Davis or Chris Garcia, Cynthia Velasco, Dennis Worth or Patrick Fisher, Shridhar Samaga, Shane Hansen

Rolls and Responsibilities

- ▪ Team Coordinator – Shane Hansen
- ▪ IVR – Chris Garcia
- ▪ ICM – Dan Davis
- ▪ WFM – Cynthia Velasco
- ▪ Witness – Dennis Worth/Patrick Fisher
- ▪ Ensemble/ECM – Shridhar Samaga

Team	Task Time
Database Administration	120 minutes

Prerequisites	Tools
▪ Disable/stop all jobs that may run during deployment window ▪ Disable Oracle services	▪ Citrix ▪ Windows Event Viewer ▪ SQL Enterprise manager
	Dependencies
	▪ All SQL servers are patched

Procedures

After 9:30

Receive 2 emails from Server Team

▪ Critical applications completed
▪ Non-critical applications completed

Perform system test on:

▪ 2 oracle servers
▪ 5 SQL servers (SQ5, SQ2, PRD, RM1, DW1, N35, N29)

Ensure database servers are operational

▪ No error messages

Enable and run production jobs

▪ Use SQL enterprise manager tool
▪ Enable Q/A test login

Conference Call to Q/A

▪ Inform team that database servers are ready for test

Rollback Contingency

▪ Receive communication from Q/A and reverse procedure

Rolls and Responsibilities

▪ Ensure all database servers are operational by checking error messages and ensuring all databases are online

Team	Task Time
Desktop Support	90 minutes

Prerequisites	Tools
Review and evaluate the pertinent patch and Smoke Test results	~~~~~
	Dependencies
	~~

Procedures

Create the Scheduled Tasks in LANDesk to deploy the patch
- Used the quiet and no reboot switches for the patch

Test the install and patch on test workstations
- Verify deployment and functionality

Copy patch to all production branch servers
- \oomc.root\install\service packs\hotfixes\<patch name>

Select the workstations applicable in LANDesk and run the Scheduled Tasks

Continuously patching workstations that did not get the patch installed from the initial deployment or that are new

Rollback Contingency (if applicable)

Rolls and Responsibilities

- Implements patch for all desktop and laptop computers.
- Download from LANDesk server
- APM creation / Scheduled task Creation
- Smoke Test
- Application Compatibility Test
- Enterprise Deployment

Team	**Task Time**
ERP (PeopleSoft)	20 minutes

Prerequisites	**Tools**
Assess server & define targeted servers ▪ 15 production ▪ 12 Dev/Test	▪ Citrix ▪ PCAnywhere
	Dependencies

Procedures

Before Test Start

Bring down PeopleSoft processes
▪ Application and batch servers

Login to servers and select shutdown

Inform Server Team of completion

9:30 Start

Server Team rolls out patch and reboots servers

Server Team informs PeopleSoft Team via cell phone that patch has been applied

Restart all application and batch servers

Login to PeopleSoft and perform cursory smoke test
▪ Look for data connection and non-cached data
▪ Ensure connection to database

Send email to Server Team that patch in working properly

Rollback Contingency
▪ Email server team that servers are not responding correctly and reverse the above procedures

Rolls and Responsibilities
▪

Team	**Task Time**
Information Security	Varied

Prerequisites	**Tools**
Receive patch bulletin from Microsoft and other software vendors	NA
	Dependencies
	▪ None

Procedures

Monitor all security vulnerabilities from trusted sources

Evaluate security vulnerabilities as it become known

Prepare summary document of all security vulnerabilities

Inform Patch Management Committee of all known security vulnerabilities

Rolls and Responsibilities

- ▪ Advisory
- ▪ Monitors, evaluates, and inform Patch Management Committee of all known security vulnerabilities
- ▪ On Call number: (949)-795-4302

Team	Task Time
Middle-Tier	After reboot: 1 hr. to complete all servers.

Prerequisites	Tools
▪ Stop MQ Services ▪ Stop Actuate Services ▪ Server systems Patching/Reboot	▪ Citrix ▪ IP Monitor ▪ VPN
	Dependencies
	▪ SQL Servers

Procedures

Communicate via conference call to Server team

Monitor all servers and determine if running correctly

▪ Use IP Monitor for status
▪ If an application is not running correctly it is restarted
▪ Restart order is important

Communicate via conference call to QA to perform tests

Rollback Contingency

▪ If not able to clear server / application problems
▪ Communicate rollback email to teams.

Rolls and Responsibilities

▪ Bring up all application servers and dependencies.
▪ Troubleshoot any issue due to patch.

Team	**Task Time**
MUST	90 minutes

Prerequisites	**Tools**
	Dependencies

Procedures

Preparation Phase
- Work with Desktop Applications to determine patches and what is relevant to environment.

Test Phase
- Download each patch separately and run functionality tests with each computer model in inventory
- Work with Middle-Tier team to post all downloads to the FTP site
- Write download instructions for each available patch
- Work with Web Team to post download instructions to the AE website in development
- Test download functionality over all internet medias (network/phone line/air card) for download times

QA Phase
- Work with Web Team to post to the AE website in production with hidden links
- Test all links on the site to make sure all are active and working

Deployment Phase
- Work with Web Team to post all links actively
- Send email to Account Executives stating new security updates are available
- Send email communication to Corporate Appraisers

Rolls and Responsibilities

- Deploys all security patches to laptops such as AE's

Team	**Task Time**
Patch Coordinator	Varied

Prerequisites	**Tools**
Receive vulnerabilities from Information Security	Effective Communication
	Dependencies
	▪ Patch Management Committee

Procedures

Stand ready and monitor conference call communications during patch deployment

After successful deployment, collect communication and summarize for team and maintain in VSS/ Share point

Rolls and Responsibilities

Coordinator, administrator, and gatekeeper of patch management project

Schedule bi-weekly patch management meetings

Compose Agenda, Meeting Minutes, task lists

Update contact lists of the Patch Management Committee as needed

Email summary to team and coordinate patch management meeting with patch coordinator

Call meeting to discuss severity, criticality, deployment timeframe, risk
▪ Collect server exception list and server reboot list from teams.
Submit CAR

Create timeline on patch deployment

Patch coordinator creates patch deployment task list
▪ Consistent forms
▪ Includes resources, start time, contact info, Microsoft information
Email form to patch deployment team members

Team	Task Time
Quality Assurance	90 minutes

Prerequisites	Tools
■ Announcement of patch release. ■ Environment and servers being deployed for impact analysis ■ Pre-deployment meeting (define responsibilities, communication) ■ User ID, passwords/permissions to smoke test applications ■ List of excluded servers and other projects scheduled for the same night as patch deployment	■ Citrix ■ Query Analyzer ■ Rational / Clear Quest, Rational Robot ■ VSS **Dependencies** ■

Procedures

Smoke test in the order shown:

■ LPS
■ LPS Credit
■ Prospect
■ Prospect Credit
■ AU (Automated Underwriting)
■ APPS
■ Mortgage Flex (Oracle DB) – Not on the same night as LPS

Provide Results for each smoke test that have occurred

Save Smoke Test in VSS under MS Patch \ release number

Smoke Test application in Production

Provide result link upon completion of testing

Rollback Contingency

Rolls and Responsibilities

- QA Team lead attends all Patch Management meetings and is included in IT-Patch Management Outlook group.
- QA Team lead arranges for testing effort. QA Analysts will be online at the stated time. When QA is informed they can begin testing.
- Results will be communicated to core patch team and posted to QA share point.

Team	**Task Time**
Server Systems	90 minutes

Prerequisites	**Tools**
Determine if patch is needed ▪ Push back if necessary as determined in Patch Management Meeting **Assess servers** ▪ Use ECM tool to assess patch applicability, generate server list and forward to patch coordinator **Define targeted server list** ▪ Create templates based upon business need and security threat ▪ Provide a list of servers that require patching to team members	▪ Citrix ▪ ECM ▪ MOM ▪ Insight Manager ▪ NetREO

Dependencies
▪ Must be notified by Information Security

Procedures

9:30 Start

Monitor progress, trouble shoot problems
▪ Use ECM tool to show Job Page/Status
▪ Correct as necessary (patch manually, reboot machines, etc.)

Monitor server health
▪ Use tools: MOM, Insights Mgr., and NetREO to ensure systems function properly.

Rollback
▪ Assess situation and determine if patch is a failure. Communicate to teams that patch will be rolled back.

Communicate patch completion
▪ Send email to queued team standing by as determined in pre-deployment meeting (team: Middle Tier, QA, Info Security, Patch Coordinator)

Rolls and Responsibilities

▪ Implements and deploys patches in all OOMC environments
▪ Provides a list of servers and related patches for each production deployment
▪ Submit all CARs to CCB for approval
▪ Provides regular and consistent status email update to Committee before, during, and at the end of all patch deployments in all OOMC environments.
▪ Provides status reporting of servers patched/unpatched on a quarterly basis.
▪ Maintain and ensure that all OOMC servers are current with security patches, hot fixes, service packs, etc.

Team

3rd Party

Task Time

- 90 minutes

Prerequisites

2 weeks before deployment

Communicate to vendors of software patch maintenance
- Date and time is acceptable
- Assess servers
- Is the patch okay?

Define server list and create exclusion list
- Communicate to Business/Customers

Schedule resources

Tools

- Citrix
- MOM
- Net IQ
- IP Monitor

Dependencies

- Ensure the following vendors are notified

AFS Check Processing	Rakis
FileNet	MIAC (Computer Associates)
Right Fax	AMICUS
PCIWIZ	Daisy (First American)
Monarch (Datawatch – ES)	

Procedures

After 9:30

Monitor System Health & Trouble Shoot if necessary

Rollback Contingency
- Email business to see if application is working properly
- Communicate successful test completion to team

Rolls and Responsibilities

Chapter 3

The Roll of the Patch Coordinator/Release Manager

The Patch Coordinator's duties require them to maintain constant diligence and a proactive stance with all business units before, during, and after a patch deployment. Along with this, the technical skill set must be broad and cover several areas of expertise. Below are a few requisite attributes:

Skill Set

- Excellent coordinator with project management experience
- Outstanding communicator
- Must remain onsite while patch is deployed
- Knowledgeable of the patch management lifecycle for each team

Tools

- Discovery building access
- Citrix
- Resource List
- This guide
- Escalation list
- Application / server list (from deployment meeting)
- Email communication
- Share Point
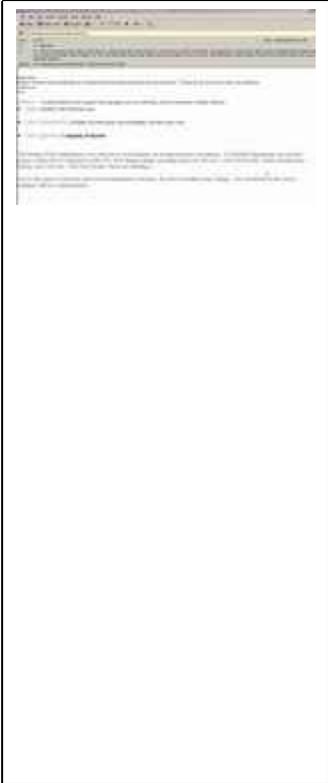- Visual Source Safe

Required Resources

- Has inventory of all machines
- Collects server lists to be patch from teams at pre-deployment meeting.
- Creates a list from this previous info and server patch order is deemed from type of vulnerability.
- Use ECM and LANDesk Tool
- Data must be collected in an organized manner (MS Excel)
- Creates a task list for deployment (includes resources, start time, contact info, Microsoft info)
- Communicates via message forum, cell phone, email

Required Documentation

In the course of the Patch Coordinator's duties, several documents must be created and forwarded to the Committee. Accurate and timely communication is vital to successful patch deployment. All documentation can be found on the patch management website on the IT Portal.

	Type	What it is
	Meeting Agenda	This document is used to communicate the purpose of the meeting, and the upcoming items of discussions for the bi-weekly meetings. This document is usually available two days prior to the meeting.
	Meeting Minutes	This document is used to capture all conversation and discussions of the bi-weekly meetings. This document is completed and posted on Share Point two days after the meeting.
	Pre-Deployment Task List and contact list	This document Is used to define agreed upon server list, task list, resource allocation, and other details related to the patch deployment. This document is completed after the pre-deployment meeting. All decisions are finalized after this document is sent out. Any changes to the finalized document require written business justification and approval from CCB.
	Post-Deployment Minutes	This document is used to document the team's actions during rollout if a patch failed to rollout successfully. Discrepancies are noted for future reference. It can also be used as lesson learned.

	Lessons Learned	This document is use s to document key items discovered during the rollout. It could also be use to log desirable or undesirable events that occur during patch deployments. Lessons Learned allow Committee to fine-tune patch management processes and help increase efficiency and effectiveness.
	Help Desk Communication Emails	This document is used to inform OOMC associates that there will be a patch deployed on a certain date, how long it will be down, and systems affected. Created by patch coordinator and sent by the Help Desk Team. Patch coordinator informs Helpdesk of patch details (date/time/affected applications/completion status). **Scheduled System Maintenance** -This email is sent two days prior to patch deployment in Production. Therefore, if the deployment is scheduled for Thursday, the notification must be sent starting on Wednesday evening, and again on Thursday evening. **Update Scheduled System Maintenance** –This email is use to provide an update communication when the patch team requires more time to complete the deployment or is running into issues. **Completed System Maintenance** - This email is sent out immediately after the successful completion of the deployment.

Location of Documentation

All patch related documents will be listed on OOMC's patch management Share Point site. This will be the common repository for future reference and patch history.

Alternate Coordinator

To minimize impact on the teams and to eliminate any coordination confusion during deployment, an alternate Patch Coordinator will be listed. This person will be called upon only when the primary cannot perform their duties due to illness or grave emergency.

Remote Patch Deployment

Before a team ever deploys a patch, the team lead will decide who are the primary and secondary team members required to perform the actual patch rollout and if it requires a person to remain at OOMC or if the patch can be deployed remotely.

Common Patch Deployment Tools

- PC with a broadband connection
- Passwords/access for applications
- Email communication from patch coordinator which states the order and sequence of patch deployment events
- Server patch list/exemption list
- Escalation/Phone list

Team Specific Tools

Critical tools that are needed for each team are shown in the Task Tables section at the beginning of Chapter 2.

Contact Information

A listing of all patch deployment personnel is attached to the Pre-Deployment email.

Patch Coordinator Time on Task

Below is a list of tasks that the Patch Coordinator performs as normal every day duties along with *approximate* time on task. Times will vary due to severity of patch.

Tasks	Estimated Time Required
Recurring Tasks	
Schedules bi-monthly patch management meetings	Minimum 4 hours; max 7 hours/week
Create/Email/Post Agenda for meeting	
Compose meeting minutes and post on sharepoint	
Facilitates all patch related activities	
Act as liaison to all IT and business units; communicates all patch related activities	
Update and manage list of servers from all teams	
Update and manage list of resources from all teams	
Coordinate schedules for patching DEV, Staging, TST, Production, etc.	
Communicates all patch related activities and changes	
Ensure that the committee is committed to following the standards and procedures set forth	
Run committee meetings and plan for activities	
Follow-up with all IT and business units for status updates	
Follow-up with all IT and business units when certain patch had been postponed, or there were issues with the deployment, etc	
Pre – Patch Deployment	
Coordinate with Team to validate resources, server lists to be patched, approval	Minimum 4 hours; max 8 hours/week
Verify correctness of server list and resources' contact information	
Gather complete server lists to be patched for the scheduled date	
Compose/send/post task lists in order of priority and sequence	
Send out communication template to Help Desk to inform business of patch deployment activities	
Send out pre-deployment communication memo to all those affected by Patch	
Review roll-out plan for correction and clarification, review time & resource constraints, dependencies, etc.	
Patch Deployment Evening – 9:30pm – 2:30pm (Approximate)	Minimum 3 hours;

Facilitate the activities of patch from start-to-finish	max 6 hours/event
Communicates with all Teams to provide status update to make sure task lists are finished according to priority and sequence	
Resolves all communication conflict and any misunderstanding of tasks, servers, or resources	
Escalate to management as necessary	
Makes diplomatic decisions as necessary (know when to call it quits or to roll-back, etc)	
Post – Patch Deployment	
Send out communication template to Help Desk to inform business of completion of patch deployment activities	Minimum 2 hours; max 3 hours/week
Send out communication email to patch mgmt committee of success/unsuccessful of patch activity	
Gather and log information from patch evening to see if any servers were excluded, had issues, had to be postponed, etc.	
Develop lesson learn from every patch deployment night	
Provide detail logged of events from the night of the patch and communicate to committee	

Appendix A

Software Update Terminology

The following table lists the new Microsoft standard terms for software updates, effective June 30, 2003.

> **Note**: The term *patch* is no longer used by Microsoft to describe a software update, except as part of the term *security patch* or when describing the process of *patch management*, which is a well understood term in the software industry.

Term	Definition
Security patch	A broadly released fix for a specific product addressing security vulnerability. A security patch is often described as having a *severity*, which actually refers to the MSRC severity rating of the vulnerability that the security patch addresses.
Critical update	A broadly released fix for a specific problem addressing a critical, non-security related bug.
Update	A broadly released fix for a specific problem addressing a non-critical, non-security related bug.
Hotfix	A single package composed of one or more files used to address a problem in a product. Hotfixes address a specific customer situation, are only available through a support relationship with Microsoft, and may not be distributed outside the customer organization without written legal consent from Microsoft. The terms QFE (Quick Fix Engineering update), patch, and update have been used in the past as synonyms for hotfix.
Update rollup	A collection of security patches, critical updates, updates, and hotfixes released as a cumulative offering or targeted at a single product component, such as Microsoft Internet Information Services (IIS) or Microsoft Internet Explorer. Allows for easier deployment of multiple software updates.
Service pack	A cumulative set of hotfixes, security patches, critical updates, and updates since the release of the product, including many resolved problems that have not been made available through any other software updates. Service packs may also contain a limited number of customer-requested design changes or features. Service packs are broadly distributed and tested by Microsoft more than any other software updates.
Integrated service pack	The combination of a product with a service packs in one package.
Feature pack	A new feature release for a product that adds functionality. Usually rolled into the product at the next release.

FAQ

Q: How are we going to disseminate this information?

A: The IT Portal web site has a link under the Operation's Main link.

Q: Why is Patch Management important to OOMC?

A: It is a core component of Risk Management. Therefore, it behooves OOMC and its associates to be proactive and diligent in assessing security threats and vulnerabilities and deploying patches.

Revision History

Date	Revision No.	
12/24/2004	Initial creation	Brian Day/Cuc Du