Situation

Is everything in place for a successful deployment of Windows® 7?

Action Plan

Taking advantage of the features in Windows 7 requires coordination between IT and business end users. Ensuring that everyone in your organization is ready for Windows 7 is a two-step process: First, create a **deployment plan** to guide your deployment, and then conduct a **Release Readiness Management Review** to reach a go/no-go decision from all affected groups before launching the deployment. This action plan assumes that each of the following has already occurred:

♦   Planning for phased deployment has been completed.

♦   Testing has been completed.

♦   Hardware compatibility and device drivers have been confirmed.

♦   Application compatibility has been confirmed.

Prepare for Deploying Windows 7

Give some thought to the following as deployment plans are prepared. Taking advantage of the features in Windows 7 may require some adjustments to established processes in IT and some preparation by business end users. Following is a list of general areas of concern and corresponding questions that affected groups should consider when implementing Windows 7:

⇒   **End-user communication.** How will the timing for the deployment be communicated to end users? What impact will deploying the features of Windows 7 have on what they do?

⇒   **Processes and policies.** How will current processes and policies be affected by Windows 7? Will old processes need to be retired or replaced? How will increased automation affect processes for monitoring, improving performance, or maintenance activities?

⇒   **Security and compliance improvements.** How will deploying Windows 7 improve security and compliance? What effects will these changes have on internal controls?

⇒   **Additional training for IT.** What training does IT need on the features of Windows 7 and how to use them?

⇒   **Operations and support systems.** Which operations and support systems are already in place and ready for deployment and which ones need to be upgraded?

The following table relates specific Windows 7 features with the stakeholders most likely to use the feature and asks detailed questions about its use.

Windows 7 Feature	Stakeholders	Key Questions for Your Organization
User Account Control (UAC)	Security team, compliance, user account management team, help desk	What user account settings in place today should change to respond to Windows 7 features? What workarounds can be replaced by new features? What procedures in place today need to change in order to use the User Account Control feature of Windows 7? Does this change new user setup? Does this change user account shutdown? Does this change user account change processes or approvals? What applications are installed that may need to be updated or replaced due to the security improvements with User Account Control? Do applications require administrator privileges for users? Do you need additional security groups? Does the enterprise have required tools, processes, and policies to support and maintain desktops where users do not have administrator privileges? Is the help desk prepared to answer user questions?

Windows 7 Feature	Stakeholders	Key Questions for Your Organization
Windows 7 lockers: BitLocker® To Go (protection of USB devices) and AppLocker (protection of applications)	Security team, compliance, help desk, travel support, field personnel, users of applications covered by AppLocker	What is your policy for requiring use of BitLocker To Go and AppLocker? How will this policy be monitored and enforced? Who needs to know about this policy, and how will they be notified? What is the policy and procedure for restoring access to locked USB devices? Are processes in place to support this? (Key backups, etc.)
Internet browser security using Internet Explorer® 8	Owners of intranet and Internet sites, security team, help desk	Do your internal and external sites work as desired with Internet Explorer 8? Are help desk procedures and troubleshooting instructions updated for when users have questions? Do the Internet Explorer security settings that are standard for the organization need to change? (See the Security Compliance Baseline Solution Accelerator on page 4 for guidance on compliance settings.)
Advanced logging capabilities including centralized logging of all event log entries	Operations, auditors and compliance officers	What logging is needed for compliance? What logging is needed for early detection of operations problems? What logging and other monitoring and control activities can now be replaced or retired? Do you have sufficient storage for increased logging?
Virtual PC and Windows XP Mode for application compatibility	Operations, help desk, end users	What commonly used applications in your organization need to run under Virtual PC or Windows XP Mode? What training, job aids, and knowledge base updates are needed to support this? What are long-term plans for retiring or updating applications that require these accommodations? Should you be using Windows XP Mode or MED-V? (See the App-V and MED-V IPD guides on page 4 for more information.) Do you have the capacity to manage more than one operating system per user?
Windows 7 integration with Windows Server® 2008 R2	Operations	How will DirectAccess be used? How will BranchCache be used? How are you managing DirectAccess and BranchCache?
Enhanced Power Management	Facilities, operations	How can IT take advantage of Enhanced Power Management capabilities of Windows 7? Does this replace other power management solutions?

Create a Deployment Checklist

To ensure a successful deployment, create a deployment checklist. Be sure to clearly define who is responsible for each item on the checklist. The subsequent Release Readiness Management Review will use the deployment checklist to confirm that these plans are in place and ready to use. Following is a list of components that should be included in the deployment checklist:

⇒ **Operations support guide.** Provides the information needed to prepare operations, service monitoring and control, customer service, and problem management teams and systems for the upcoming change.

⇒ **Deployment and contingency plans.** Includes deployment goals, critical success factors, deployment tasks, resources, and tools.

⇒ **Security implementation plan.** Describes how the service will be brought to acceptable levels of security. It details existing security threats and how implementing security standards will mitigate those threats.

⇒ **Risk management plan.** Contains an analysis of likely risks with both high and low impact, as well as mitigation strategies to help the project avoid being derailed should problems arise. Identify both the deployment risks and the operations risks for the project.

⇒ **User acceptance approval.** All key stakeholders confirm readiness of components and agree to proceed with deployment. Evidence of the approval should be retained for the project and stored with project materials for subsequent audit reviews.

Conduct a Release Readiness Management Review

The focus of the Release Readiness Management Review is on determining cross-team readiness for deployment. Participants in the Release Readiness Management Review include representatives of the operations and support teams, the project team, the security team, and business end users. Participants must be empowered to make decisions at the meeting.

The Release Readiness Management Review occurs near the completion of the engineering work, between testing and deployment. It's a comprehensive review of the deliverables produced, as well as an assessment of the readiness of the business to employ this solution and of IT operations and support readiness to take over responsibility for this solution in the production environment.

In the Release Readiness Management Review, the team evaluates four aspects of release readiness:

♦ Operability and support of the release

♦ Readiness of the production environment, including the organization and infrastructure, to support and operate the release

♦ Readiness of the business to use new features and functionality

♦ Readiness of the release strategy plans, including rollout and rollback plans, training plans, and support plans

The Release Readiness Management Review results in a go/no-go decision about whether to deploy the release. Having clear criteria in place that all participants of the Release Readiness Management Review understand and agree on is fundamental to effective decision making.

The following table provides a quick summary of indicators that can be used for the go/no-go decision.

Element	"Go" Indicators	"No-Go" Indicators
Release	All prerequisites have been met. All documentation is in order. Adequate rollback plan exists.	Release is not built to standards. Documentation is missing. Primary and secondary support personnel have not been assigned.
Production environment	Support staff has fundamental understanding of the technology and of the changes being made. All administrative procedures for the release are clear and aligned with site standards. Operating level agreements (OLAs) and underpinning contracts (UCs) are in place and appear to support required service levels.	Software or infrastructure levels used to build the solution are unsupported (too new, too old) in the current environment. No support staff training plan. No backup plan.
Release strategy plans	Escalation process and contact list have been communicated. All key stakeholders have been notified. All resources required for implementation have been confirmed.	Single point of failure or fatal flaw exists in plan—for example, dependence on one technician. Plan prerequisites have not been met, such as confirmation that users will be on hand to do acceptance testing. Change management documentation is not in order.

Learn More

This **real-life IT solution** was brought to you by Microsoft Operations Framework (MOF) 4.0.

To learn more about the free, practical guidance provided by MOF 4.0, visit **www.microsoft.com/MOF**.

Download related content:

⇒ **Deploy SMF.** This service management function is useful for anyone who is involved with releasing a stable IT service solution into the production environment, including stabilizing the solution in the production environment and transferring responsibility for the solution from the Project team to the Operations and Support teams.

⇒ **Release Readiness Management Review (Deliver Phase Overview).** This guidance represents a comprehensive review of the deliverables that were produced, as well as an assessment of the readiness of the business to employ this solution in its work and of IT operations and support readiness to take over responsibility for this solution in the production environment.

⇒ **Microsoft Operations Framework (MOF) 4.0.** Microsoft Operations Framework (MOF) 4.0 incorporates the core requirements of industry best practices and frameworks into one, free, easy-to-understand set of guidance. MOF provides practical recommendations that IT pros can immediately apply to solve business-critical challenges.

⇒ **Microsoft Assessment and Planning (MAP) Toolkit.** Use this network-wide inventory and assessment toolkit to determine if your existing PCs meet the hardware and device compatibility requirements for Windows 7 migration.

⇒ **Infrastructure Planning and Design (IPD) Guides for Virtualization.** Use this authoritative design guidance and its step-by-step approach to better and more quickly plan for a new desktop virtualization infrastructure that is based on App-V or MED-V virtualization products.

⇒ **Windows Optimized Desktop Scenarios Solution Accelerators.** Use the assessment tool and planning guidance to gather desktop user requirements and align them to available Windows Optimized Desktop technologies such as Windows 7, DirectAccess, MED-V, App-V, and more.

⇒ **Microsoft Deployment Toolkit (MDT) 2010.** MDT unifies tools and best practices into a common deployment console and collection of guidance enabling you to efficiently and cost effectively deploy Windows 7 and Windows Server 2008 R2 across your organization.

⇒ **Security Compliance Management Toolkit Series.** Meet security and compliance requirements with the Security Compliance Management Toolkit Series, now updated with baselines for Windows 7 and Internet Explorer 8.

Microsoft Solution Accelerators

Microsoft Operations Framework and the related content listed above are all offerings from **Solution Accelerators**.

Solution Accelerators are authoritative resources that help IT pros plan, deliver, operate, and manage IT systems that address real-world scenarios. Solution Accelerators provide free, prescriptive guidance and automation to accelerate cross-product integration, core infrastructure development, and other enhancements.

www.microsoft.com/solutionaccelerators