mPower Standardized™ Desktop Lifecycle Management

A multi-layered approach to delivering a true universal OS and single image technology.

mPower Whitepaper
Mark A. Buscaglia
Chris Rocca

mpower SOFTWARE SERVICES

Introduction

mPower Standardized desktop life cycle management methodology is a framework designed to resolve and manage the internal challenge corporations are facing today – The inability to consistently obtain, deploy, manage, and reclaim business assets – including software licensing, hardware, user ID's, employee credentials and/ or any critical data or asset necessary to introduce and maintain corporate human capital.

The maintenance of this data is not just "an internal challenge" to corporations but rather a requirement. Thousands of public facing companies are tasked to ensure their accounting and business operations are in compliance with governing policies like the Sarbanes Oxley Act.

Private companies face similar requirements; for example, the Gramm-Leach-Bliley Act for financial institutions and Health Insurance Portability and Accountability Act (HIPAA) for companies operating in the healthcare industry.

In addition, financial auditing departments must not only provide a comprehensive external financial audit, but they are also subject to a multi-source compliance specialist audit to identify areas of operational risk. These examples represent some of the requirements and regulations that can have significant financial and operation cost impact on the implementation and management of an enterprise IT environment; specifically related to desktop management (access, reporting, data storage, etc).

This document speaks to the process methodology that manages the design, implementation and delivery of a standardized technical framework which can deliver a managed desktop lifecycle environment. The functional frameworks which make up the mPower Standardized desktop life cycle management methodology and the critical role of BDNA Discover and BDNA Normalize in the application rationalization phase are discussed. In addition, this document focuses on the subsequent steps used to deliver a more effective approach for desktop standardization and management, while providing a solid desktop foundation for simplifying large scale IT projects including Windows 7™ migrations, technology refreshes, vendor audits, device standardization and IT cost reduction initiatives.

> *"Deliver a more effective approach for desktop standardization and management, while providing a solid desktop foundation for simplifying large scale IT projects."*

The Problem

Complex IT Challenges

Today, IT client support organizations find themselves in the difficult situation of accommodating necessary technology implementations such as Windows 7™ migrations, hardware refresh cycles, inventory true-up's and small peripheral implementations including iPads and Slates, while under the direction to reduce desktop service support costs without impacting end user production.

The myriad of client facing technical support issues that enterprise business organizations must address can lead to environments which function, but are not efficient, cost effective or truly cohesive. This is often true even after efforts to implement basic single image solutions. Despite diverse businesses models and industries, the most common IT challenges are nearly universal and add layers of complexity to implementing a single image approach to desktop lifecycle management.

- Multiple PC images
- Non-standard hardware and software
- Inefficient hardware deployment processes
- Reactive service desk and support backbone
- Non-compliant software in the business environment
- Unsecured network devices
- Unknown applications in the business environment
- No clear data management capability

To understand the tactical and financial impact needed to accomplish these goals companies must leverage and rationalize the smallest available data points located on the greatest common denominator of an enterprise business organization – the desktop.

The Solution

mPower Standardized™ a Unique Approach to Desktop Lifecycle Management (DLM)

One of the most widely accepted practices for standardizing a desktop environment has been the adoption of a single universal image – 1 operating system which supports all enterprise hardware. While the single image is a good first step toward standardizing an enterprise desktop environment, there are limitations on cost reduction and the simplification of technical support services. But, if properly developed, a single image can form the foundation for the implementation of peripheral "horizontally functioning" desktop standardization efforts. These include managed application and patch deployment, automated desktop management, automated PC build and reimaging processes which create a unified approach to desktop management.

mPower Standardized™ methodology is an approach to Desktop Lifecycle Management (DLM) that seeks to achieve the goals of using the right technology for the right task, simplifying that technology design, easing its maintenance, fitting those technologies together in a complimentary fashion, and using the combination of technology and processes to gain efficiency and drive cost savings in the following areas:

- Enterprise organizations must plan for dramatic gains in operational efficiency
- Create significant measurable cost savings – support service cost reduction
- Reduce audit risk – software licensing, access compliance, financial controls
- Reduce technology footprints – less technology equals less man power
- Establish a forward compatible technology platform

mPower Standardized™ differentiates from other DLM methodologies with a combination of tools from BDNA, analysis of both technical and business processes, and a unique layered approach to building a universal OS and single image.

What is mPower Standardized Desktop Lifecycle Management?

Framework Overview

Desktop Lifecycle Management (DLM) is the implementation of a strategic solution that will enable the desktop enterprise management of one user, one identity, one infrastructure. Tasked with a common set of business and technology data management regulations and requirements, many corporations are looking to implement a reasonable strategy for proactively managing their desktop IT and financial business environment.

mPower Standardized™ solution to desktop lifecycle management implementation is carried out through 5 distinct delivery frameworks:

mPower Standardized™ 5 distinct delivery frameworks:

1. **Universal Image** – standardize and automate the operating system
2. **Application Library** – organize, automate, and manage applications
3. **Delivery Toolset** – centralize deployment of applications and settings
4. **Management Hierarchy** – organize and manage the alignment of roles and their corresponding application resources
5. **Security Controls** – protecting company assets and information

Universal Image (Standardize and Automate the Operating System)

An operating system (Windows XP™, Windows 7™) that is preconfigured, automated and then encapsulated into a process that can be deployed to all desktops, laptops and tablets regardless of their hardware (Dell™, Lenovo™, HP©, etc.)

Application Library (Collect, Analyze, Normalize and Manage)

A collection of software installations that are broken down and then reassembled into single packages which can be installed on any workstation. These application packages are fully automated eliminating any prompts that are normally required during the setup process (i.e. license agreement, shortcuts, configuration settings, etc.) Depending on the requirements and infrastructure, applications can be packaged either physically (MSI installations) or virtually (virtual applications). Once an MSI is installed, the application can protect itself by "self-healing" if suddenly alteredor damaged. Virtual applications are typically even more robust, in the event that functionality issues arise, they need only be restarted to restore themselves back to their original state.

Delivery Toolset (Stabilize, Centralize and Deploy)

The toolset (i.e. SCCM, LANDesk, Marimba, etc.) which delivers application packages, patch updates, policies and rules to apply to the workstation and the end user.

Management Hierarchy (Organize, Align and Manage)

A hierarchical alignment which associates the MSI or Virtual application library with functional and operational roles within the organization (i.e. Microsoft Active Directory). Centralized policies can be applied to each workstation. Every business department has their own container where applications, security patches, service packs and policies are associated (i.e. A member of HR automatically receives a software application called PeopleSoft© and a policy that changes their desktop wallpaper automatically). This allows ease of management for the deployment and reporting of assets: applications, patch updates, application access/ permissions, machine names, business locations, etc.

Security Controls (Protect and Report)

The implementation of security controls across the organization, protecting workstations from internal and external threats (i.e. antivirus, patch and spyware management, VPN, software firewall, user authentication, etc.)

> *"Develop a cost effective common infrastructure (and supporting process) from which the various corporate assets of the DLM cycle can be launched, centrally configured, managed and reported."*

Understanding Standardized Functional Components of the 5 Delivery Frameworks

mPower Standardized™ Desktop Lifecycle Management

Each Management Framework is comprised of five overlapping "Vertical Functional Components" and the supporting "Horizontal Business Process" to implement the managed end state. The implementation of the functional and business process components enable cross departmental data exchange, robust management and reporting capability. Many technical components like configuration scripts, OS and patch updates or packaged applications cross the different Vertical / Functional Components (desktop, Windows Server, Exchange, Systems Administration, etc) of an IT business operation. Each of these tactical components carries a varying degree of financial and operational impact on a typical business enterprise environment.

The mPower Standardized™ implementation methodology for delivering a standardized technical environment begins with the standardization of the end user desktop. This methodology is born out of business best practices and implementation standards for enterprise level IT business support organizations. The solution is based on years of first hand desktop and network management and industry standard best practice experience. It relies on mPower's end user management experience to design and implement a client's infrastructure technological solutions. These solutions have enabled mPower clients to benefit from a centrally managed, functionally independent systems framework, which results in a workstation environment capable of:

Self-Assembly

Self-Assembly allows technicians to build multiple workstations at the same time thus drastically reduce PC build times- leading to less end user downtime and quick turn around on provisioning cycles (new hires, upgrades, projects, etc.)

Self-Configuration

Self- Configuration automatically assigns certain (scripted) values to new PC builds that are traditionally manual and time consuming: assigning PC names, user names, etc.

Automated Security Baseline Management

The "baseline" or required security settings are pre-scripted within the image thus removing the need to manually set required security levels on a per machine basis: this speeds up build cycles and removes the possibility of manual error

Application Fault Tolerance (Self-Healing)

Packaged Microsoft Installer (MSI) or virtual applications provide application fault tolerance. This will allow business applications to "self-heal" themselves if an end user or another application inadvertently breaks or removes critical settings or files.

A good example would be an end user who inadvertently deletes critical files from his/ her Adobe Reader application. Rather than having to experience an application failure (triggering a first call incident report and requiring second level escalation to desktop support) the application will "self-heal" and the individual will not experience any failure (the incident will be transparent to the end user- a non- event).

This is a simple but typical example of a proactively resolved incident which leads to the drastic reduction of operational support costs and maintenance complexity.

Above the Vertical Functional Components and the Horizontal Business Processes are further defined for implementing each of the 5 Frameworks:

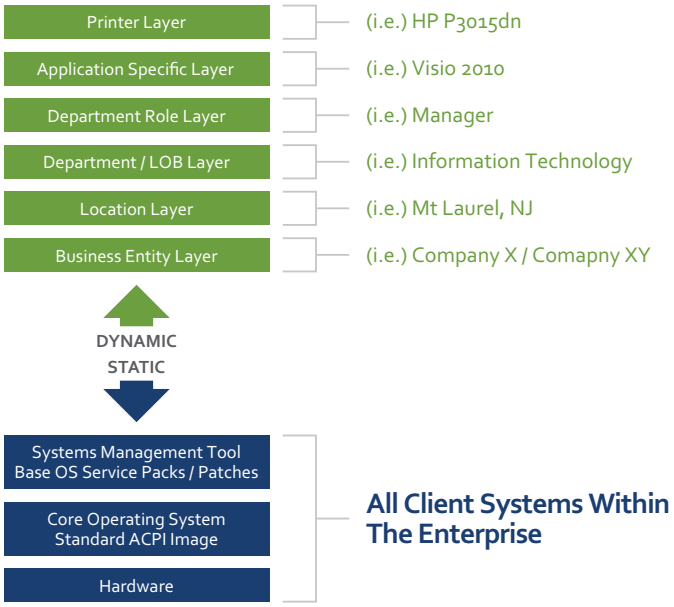
The Universal Image

mPower Standardized™ leverages the 5 step Standardization Framework to develop, test, validate, and deploy a single image / operating system (Windows XP™, Windows 7™) to all workstations regardless of their hardware (EXAMPLE: Dell™, IBM®, HP©, etc.). The single image build process takes into account, but is not limited to, hardware driver solutions and "Client - specific" requirements applied to the following build elements:

- Test/integration lab
- Unattended installation
- Sysprep configuration
- Image creation

The widely accepted standard for provisioning and managing workstation operating systems and application load sets is based on a modular, layered approach, which begins with a relatively small "single image". Thanks to the multi-vendor backed hardware standards, a single image can work on all workstations regardless of the specific hardware configurations. Application packages are developed and installed atop the single or universal image.

In addition to saving considerable time within the Test/Integration Lab, this eliminates hardware problems when new applications are installed and thereby reduces the number of steps in the QA process. The following graphic illustrates the single image coupled with the 4 other Frameworks which mPower Standardized™ deploys to standardize the client's PC environment.



Application Library

Standardization and Library Creation

The next logical layer in the standardization process is to discover, rationalize, and review the applications that exist in the enterprise. This can be a daunting task as gathering accurate and timely information can be challenging. Use of the appropriate tools, such as BDNA Discover™ and BDNA Normalize™ can increase the speed at which data is gathered, and greatly enhance the accuracy and usability of the data. This process allows the creation of a list of accepted applications in the environment that can be packaged to allow reliable, durable, consistent deployment to end users. mPower Standardized™ accomplishes this process through the following:

Application Discovery – Identification of all production applications running within the business enterprise

Application Rationalization – Confirmation, rationalization and tactical review of the application discovery data.

Application Packaging (Library Configuration) – Configuration of application media into an MSI or Virtual package.

Application Discovery

mPower Standardized™ uses the BDNA Discover™ and BDNA Normalization™ to perform a comprehensive application data discovery, normalization, and analysis of the application environment. To do this, mPower uses an SCCM extract file from the client's SCCM environment. The value provided by normalizing raw data (collected by BDNA discovery solutions – SCCM extract file) in a matter of hours will enable mPower to quickly and accurately establish the application library standardization effort. Through a partnership with BDNA, mPower has integrated these tools into mPower Standardized™ to gather this data faster and with greater accuracy than other methods, saving clients time and money in this process.

IT Visibility Tools Provided By

BDNA

www.bdna.com

Application Rationalization

Once the BDNA Normalize™ output data has been gathered an mPower analysis can be done to obtain a true picture of the environment which is often far different and expansive than most managers realize. One of the greatest attributes of the BDNA sourced data is the way the data is rationalized which takes massive amounts of information and distills it into much more usable data points. This step often causes a great deal of difficulty for organizations using conventional tools as they are often faced with an overwhelming amount of data with no easy way to handle and organize it. The typical effort is often too much which frequently leads organizations to only complete part of this process, or skip it altogether. But without this data organizations will have a difficult time finding their most widely used applications, their versions, and usage.

Application Packaging (Library Configuration)

As a progression of the application rationalization phase, mPower guides the client through the Application Library Implementation Phase. mPower will work with the client to designate a number of applications for automated packaged deployment. The application packages are a practical combination of available technologies: MSI and/ or APP-V Virtual Applications. mPower determines packaging formats (MSI, Virtual, etc) based on a sampling of critical environmental end user variables such as; number of users, application function and end user access points / usage.

Establishing the Application Library

mPower Standardized™ begins the application library definition by establishing core application groupings:

- Core Level Applications
- Enterprise Level Applications
- Department Level Applications
- Individual Level Applications

These technical application standards establish a hierarchical structure from which all internal corporate departments benefit from increased production, decreased maintenance and greater operating efficiencies / or lower costs. The establishment of enterprise-wide standard applications can be viewed as a mechanism for optimizing technological resources such as desktop support staff and service center resources.

> *"All internal corporate departments benefit from increased production, decreased maintenance and greater operating efficiencies / or lower costs."*

By categorizing applications into pre-defined groups, we are establishing the foundation for an expedited provisioning mechanism; maximizing the use of tactical human resources which creates a measurable reduction in ongoing application management and deployment costs. This automation process uses fewer man hours yet yields faster, and crucially, more consistent application delivery to end users. This structure of applications can then be used to optimize the license management process for the organization's applications.

Requirements Definition and Analysis

This is the key phase to building an Application Library. The mPower team gains a comprehensive understanding of the client Packaging Requirements through a series of internal interviews. The primary objective during this phase is a completed application packaging requirements document.

To ensure the final product meets the client functional requirements, mPower develops a test strategy and defined test scenarios and conflict checking process. Additionally, mPower will finalize the Packaging Lab / Development environment.

Packaging Development

mPower's Application Packaging team will now begin the application packaging process for the applications defined in the requirements specification. Each work effort undertaken is conducted under mPower quality guidelines and in accordance will all existing client standards.

The Application Packaging Process

Process the applications to be processed based on the prioritization established. For each application:

- Confirm MSI/ Virtualization Standard to be used
- Acquire the completed approved application requirement documentation
- Download the media source for the application from the client application source Library. Load this source into the mPower Application library on the server.
- Package the application per the installation requirements, configuration requirements and packaging tool to be used. This will include any Customizing of application installs to meet different business unit requirements.

- Communicate with the client should any issues arise. This may be with the designated client project lead or with the application owner directly.
- Store the package deliverable on the application deliverable folder on the server.
- All the packages will go through a quality process to ensure the package is reliable and deploys the desired client configuration with no issues.
- Document the package as required by the client and identify any known issues with the package. Track the package history as well.
- Load the completed package and documentation in the completed deliverables folder on our server. These items will then be uploaded back to the client for Acceptance testing.

Unit testing is conducted by the packagers to ensure that package is complete and working as designed. Each package is tested independently. At the end of unit testing the application package will run without abnormal termination.

The activities that occur in this phase include:

- Packaging of the prioritized applications (location, number of users, OS Conflict Checking)
- Unit testing of the packages
- Package documentation

Client Testing / Verification

This phase will involve testing of the packages. Once an application has been successfully packaged, tested and documented in our environment, the completed package will be uploaded to a designated server in the client environment.

Client resources will then be asked to execute an acceptance test. The client acceptance testing is conducted by client to ensure that the packages meet all requirements, reliability, and performance expectations in a production-like environment. Tests will mimic typical or anticipated usage patterns. Any issues that may arise will be handled through the issue management process and tracked through resolution.

The activities that occur in this phase include:

- Package deliverables staged to the client by mPower Application Architecture Team
- Acceptance Test Preparations
- Acceptance Test
- Continue with the Risk Management and Issue Management Procedures

Implementation

The Implementation Phase involves the activities for having the completed packages and documentation implemented into the appropriate environment. mPower will assist in the implementation as well as in the communications plan, support plan, roll-out initiatives.

Delivery Toolset

Once the Application Library is established the Delivery Toolset, which is the enterprise level application deployment mechanism will be put into production for application distribution and patch management. Examples of enterprise Delivery Toolsets include Microsoft SCCM, LANDesk, and Novell Zenworks. The Delivery Toolset is another key component which allows for the creation and delivery of a fully configured and automated operating system with core level, enterprise level, departmental level, and user level business applications.

“The Delivery Toolset is another key component which allows for the creation and delivery of a fully configured and automated operating system with core level, enterprise level, departmental level, and user level business applications.”

Management Hierarchy

mPower aligns and extends the managed hierarchy architecture which is associating the applications with functional and operational roles for distribution and management of end user PC's. A common example of this is using Microsoft Active Directory configured with the appropriate groups and objects to define end user departments and roles, centralized policies can be applied to the workstations based on their roles. Each business department has their own container (or folder) where applications, security patches, service packs and policies are associated (i.e. A member of HR automatically receives a software application called PeopleSoft© and a policy that changes their desktop wallpaper automatically).

Having the ability to segment application and end user profiles into assigned groups (and OU's) enables cross function access and permission management. This simplifies the ongoing support model for Level 1 and Level 2 technicians. This also further enables your Delivery Toolset to reach maximum functional capacity as it broadens usage capability for remote desktop management toolsets through Group Policy.

Group Policy - Server based applied setting to a user or computer that can manage the behavior and/or access to a device.

Security Controls

The integration of functional desktop security components and process controls mitigate internal and external threats to critical data and business systems. When implemented with enterprise policy and end user function in mind the following control points can mitigate enterprise security exposure in a cost and operationally effective manner.

Virus – Desktop utility to eliminate or mitigate external and/ or internal virus or Malware threats

Firewall – Gateway that limits access between networks in accordance with local security policy

Data Encryption – The cipher encryption of business critical user data for the purpose of keeping it confidential or private.

User Authentication – authentication tools such as Two-Factor authentication which serve to identify and verify approved users

OS level policies – can be used to restrict and "lock-down" parts of the Operating System to prevent intentional attacks and accidental end user damage.

Establishing a Scalable Technical Foundation

By implementation of these frameworks organizations can position themselves to be able to adapt, expand, and modernize their IT operations. Standardization of different areas allows a modular approach which then makes it much easier to scale up operations as required, or update to new technologies now that a solid modular foundation exists. Components can be added and removed more easily allowing new technologies or features to be introduced into the consistent, modular, and structured environment.

Service Desk: Incident Management

As an enterprise organization establishes a new desktop foundation, they will begin to track and report on cost reduction at the organizations service level. Traditional level two service escalation will be moved to first level resolution, i.e.:

Incident Management – Pinpoints and tracks the source of technical or operational incidents, allowing your service desk to correct issues quickly. Association of user IDs through directory service ties the incident history to the user and tracking of source data for technical or operational incidents (including service desk responses, SLA status and incident metrics).

Organizations will not only be able to track and associate cost reduction around incident management, they will gain the ability to target frequently reported end user incidents like password resets, etc. This will pave the way for the implementation of:

Self Help – The capability to report the metrics of provisioned tools and process to the user base to troubleshoot and solve technical issues

In addition to Self Help tool implementation, organizations will have the ability to objective analyze and implement new security initiatives like:

User Authentication – The process of determining whether someone or something is, in fact, who or what it is declared to be. Tracking authentication accuracy and metrics, user logon history, termination and new hire access, etc.

Asset Management Capability

Once an organization can reduce and rationalize its desktop incident management and reporting environment, they can refocus their resources and efforts on strategic initiatives to further reduce operating expense; specifically in the asset management discipline. We are defining Asset Management as a business discipline for managing the life cycle of organizational assets to achieve a desired service level while mitigating risk. It encompasses management, financial, customer, engineering and other business processes which we can directly relate to the standardization of an enterprise desktop environment. True asset management is not a system you can buy, but is instead a business discipline enabled by people, process, data, and technology.

We can directly improve an organizations Asset Management capability around the following desktop components:

Desktop Hardware Management – The tracking and maintenance of all requisitions, purchases, procurement and reclamation for hardware

Client Software Management – The tracking and maintenance of all requisitions, purchases, procurement and reclamation for software

License/ Asset Management – Reporting on license min max numbers, warranty expiration, amortization cycles, inventory counts, etc.

> *"Once an organization can reduce and rationalize its desktop incident management and reporting environment, they can refocus their resources and efforts on strategic initiatives to further reduce operating expense."*

Audit and Compliance Capability

Tighter security controls and regulatory reporting around data management, systems and account access have elevated the importance and associated cost of an enterprise security practice. mPower leverages improved infrastructure management byproducts of a standardization effort to further improve enterprise Audit and Compliance capability. mPower is defining Audit and Compliance as a comprehensive, systematic, documented evaluation that is designed to find and fix operational and financial violations for companies and individuals. It includes not only a compliance review, but regular reporting requirements and schedules for correcting problem areas discovered during the audit.

To manage these requirements IT organizations introduce toolsets which add a layer of complexity to the ongoing management and support of the desktop environment.

Data Encryption – Reporting and tractability of cipher encryption function of business critical user data

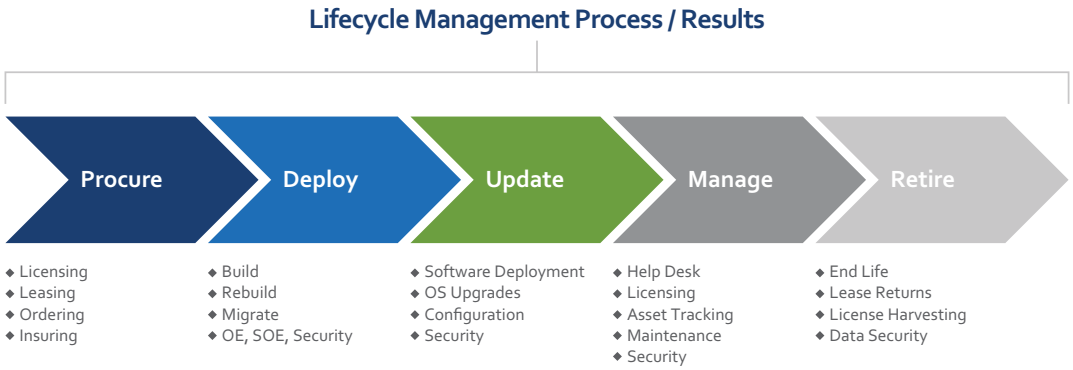
Virus – Reporting and tractability of desktop utility function and mitigation of external and/ or internal virus or Malware threats

Firewall – Tracking on functionality of user access between networks in accordance with local security policy

These tools protect the desktop (and help to manage organizational risk) but they further complicate and extend the upgrade and new build cycle of a typical desktop environment. Standardizing the desktop environment helps to better manage the security tools in both production support and ongoing maintenance scenarios by reducing build cycles, limiting access, protecting local data and systems access points and improving reporting management for ongoing audit compliance initiatives.

Conclusion: Critical Success Factors

Organizations need to understand the ongoing financial and organizational benefit of establishing a strong desktop foundation which is process repeatable and technology agnostic. To fully leverage a new technology implementation (Windows 7™, Desktop Virtualization, Mobile Tools) an organization must establish a measurable and repeatable desktop foundation which enables the organization to not only tactically serve the end user but strategically provision new cost effective, available technological business tools which deliver increased revenues. Most organizations will see immediate cost benefits from funding desktop standardization efforts during technology refresh efforts. All organizations will see holistic reduction on desktop TCO costs associated with hardware and software provisioning and support services on an annualized basis.



Organizations will see cost reduction and operational improvement around the following desktop service and provisioning areas:

Improved Audit Reporting capability

End User Account Management:

- Deliver a consistent, controlled, manageable user experience across the enterprise (operating system, applications, security definitions, policies)

Asset Management:

- Easily account for, provision, track, audit, and report all assets
- Granular monitoring and management of hardware assets to maximize effective lifecycles
- Drastically reduce over-licensing, over-spending
- Advanced software licensing methods such as license delivery and reclamation

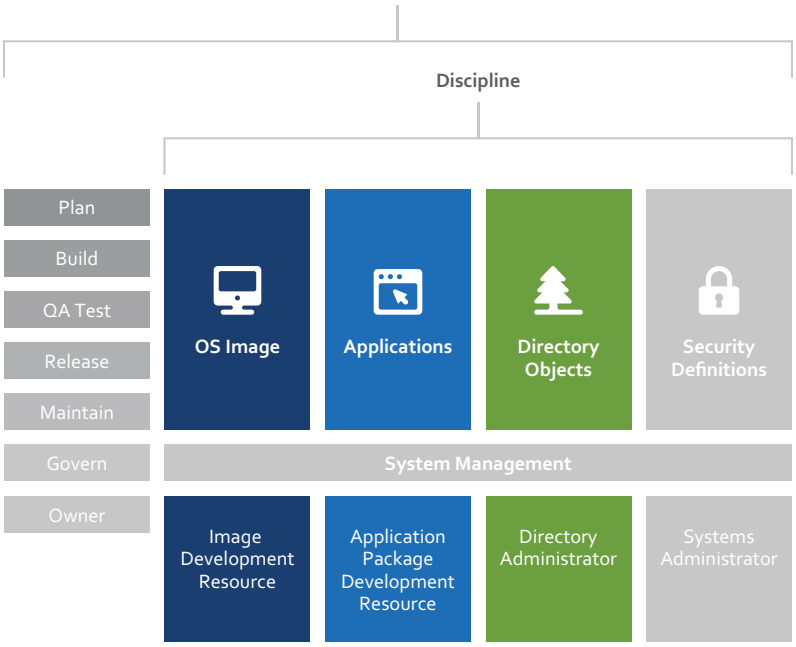
Desktop and Service Desk Workforce Optimization:

- Reduce workstation lifecycle management cost by as much as 80%
- Reduce the volume of help desk calls, desk-side visits, and associated manpower expense
- Rapidly deploy new software, patches, and hardware (improved cycle time)
- Faster problem resolution via remote control MSI self-healing and application virtualization

Disaster Recovery:

- Provides a realistic workstation disaster recovery mechanism – enabling DR workstation rebuilds and forward compatibility with new technologies (MS Windows 7™, Windows 8™ and Virtualization)

Building Your Assembly Line



U.S. Headquarters
mPower Software Services
115 Pheasant Run
Suite 110
Newtown, PA 18940
Tel: 215-497-9730
Fax: 215-497-9736
info@mpowerss.com

www.mpowerss.com

US Headquarters
BDNA Corporation
339 North Bernardo Avenue
Suite 206
Mountain View, CA 94043 USA
Tel: +1 650-625-9530
Fax: +1 650-625-9533
americasales@bdna.com

www.bdna.com