

# Web-Centric Production Acceptance

By: Harris Kern's Enterprise Computing Institute

*You've recruited, hired, trained, and retained the best software engineers, architects, and managers in the industry. You've established a world-class software development organization for these engineers to work in. You've brought the best software development tools money can buy and each developer has a top-of-the-line workstation and a private office. Your glass-house computer room is filled with high-powered file server, DBMS servers, and the latest networking gear. Your software development team has worked for months to prototype, design, implement, and test a web-centric application, assuring every user requirement is met. You've worked with the IT operations staff to put in place a Service-Level Agreement. Your long overdue vacation plans are looming on the horizon and it seems like your project is nearly complete. Surprise! There is still one more task to do before you can claim a successful web-centric software development project – a very, big task. We call it the Web-Centric Production Acceptance (WCPA) process.*

The WCPA is our most important process. Implementing a WCPA process often makes the difference between the success and failure of a web-centric software development project. We have worked with many Fortune 500 companies who have attempted to deploy web-based applications, some successfully and others ending in project failure. Many of the failures were due to the absence of a process to deploy, manage, and support distributed, web-centric applications and their supporting infrastructure across the enterprise. The WCPA started life as the Client/Server Production Acceptance (CSPA) process. We have modified the CSPA process to specifically address the requirements of developers working on web-centric applications. Like the CSPA, the WCPA is our way of transitioning applications from development to production, i.e., deployment. It's also our way of making sure customers get the same reliability and security for their globally deployed Intranet, Extranet, and Internet applications as they did with their mainframe or client/server applications. The WCPA is our way of improving and maintaining IT and customer dialogue for systems support and development. Just as web-centric is a revolutionary computing paradigm; the WCPA is our contribution to a new age of IT customer relations enabled by personalized, web-based communications.

## The WCPA Questionnaire

The WCPA process starts with a questionnaire that helps the software development team, the IT operations team, and the end user customer assess the readiness of the complete environment surrounding the deployment of a new application. When used effectively, this questionnaire is filled out during the entire development process, rather than waiting until immediately prior to deployment. The first section of the WCPA covers the operational environment the application will be deployed in:

- Hardware (CPU, memory, disk, network)
- Operating system
- Storage requirements

- Database requirements
- Job/batch schedules
- Error messages and handling

The second part of the WCPA questionnaire describes support requirements of the application, including:

- Interdependencies of the application on other jobs and systems
- Capacity planning
- Systems availability (online availability, backup windows, etc.)
- Testing plan (alpha, beta, pre-production, stress testing, and so on)
- Training of users and IT support staff
- Documentation for users, help desk staff, operations staff, etc.
- Administration processes
- Support procedures (hardware, OS, network, application, 3<sup>rd</sup> party vendors, etc.)

The third part of the WCPA questionnaire deals with exception procedures or any specialized requirements of the application including:

- Security
- System moves/changes
- Critical system messages
- File system backup and archives
- Disaster recovery

## **Personalized Communications**

The WCPA places a special emphasis on communications between the three stakeholders in a successful software development project: the developers, the IT operations staff, and the end users. From the very beginning of the process, the WCPA opens the lines of communication between all three groups. The database administrators, system programmers, production control personnel, and computer operations work closely with applications developers and end users to understand the requirements necessary to implement and support a distributed web-centric application.

The WCPA's approach of personalized communications contrasts starkly with earlier models of software development, such as waterfall software lifecycles. The WCPA is a proactive, not reactive. In the past, the only time MIS would get involved with users was when a problem occurred. Someone would call the Help Desk. The Help Desk would call data center operations. Operations would come to resolve the problem. That was and still is the paradigm in many data centers. This paradigm, however, does not work for today's web-centric applications environments. You need to work closely with your users to solve the business issues of new applications or they will never be successful, no matter how skilled your developers become.

The WCPA is responsible for setting everyone's expectations, for communicating roles and responsibilities, and for establishing how groups and individuals – customers and the data center – work together. It is a service-level agreement between different organizations. The WCPA is also the communications vehicle to ameliorate the cultural differences among Unix, PC, and mainframe personnel, applications development, IT support, users, and the data center as they come together to support web-centric projects. Personalized communications is not just a buzzword. It is a new way of doing business and working together for the benefit of the whole enterprise.

## **Internal Support Agreements (ISA's)**

Service-level agreements have long been the mainstay of mainframe production systems and larger Unix client-server systems. On the web, however, service-level agreements become much harder to define and monitor. No longer are all the components of the application residing in a glass-house data center, or even distributed within a company. Web-based applications may span multiple companies in an Extranet or, in the case of the Internet, may span across the world. The WCPA questionnaire, when filled out, helps span the many environments of the web and becomes a template for an internal support agreement between users and IT.

The internal support agreement is aimed at three groups:

- Business managers receiving IT services, who need to ensure that the services delivered are in line with their business requirements at a cost they are prepared to pay.
- The system administration staff, who deliver these services and need to fully understand the commitments that customers require in order to provide quality service.
- The new enterprise network services staff, which coordinates the delivery of these services across the web to their respective business units or external customers to ensure maximum contribution to business effectiveness.

With an internal support agreement, both internal and external customers can understand the kinds of service they should expect from their computer resources and how those resources are expended. On the other side, an internal support agreement makes sure system administration personnel understand their jobs well – what services they provide as well as those they don't provide.

The differences between applications development and operational support are well publicized and have been going on for decades. Even when development and operations were centralized under one MIS organization, finger pointing was common behavior and everyone had no choice except conform to the same rules and guidelines. Networked computing has changed all that. Most of the issues centered on implementation and support of mission critical applications. Development would blame operations for messing up a

restart or operations would blame development for lack of QA or support on their part. There were many issues of this nature.

In many companies applications development is located within the business unit or division for business reasons – this is good for quickly responding to business issues and requirements, but puts additional friction between the groups. After decentralization, companies must also deal with the cultural differences that occur. Many of the younger development staff comes from a Unix, NT, or client/server background. So now you often have Unix mentalities versus legacy culture mixed within the same development organization.

In the early days of client/server computing, development organizations would attempt to support their own servers. Today, most development organizations want centralized IT to support their servers for system administration functions such as tape backups and restores. This is not much different than the old way of doing business when operations would support the development environment on the mainframe. One of the cultural changes that must be addressed when IT takes control of development servers is ownership of “root” authority (security privileges). Development organizations without IT support often enjoy the freedom of being on their own and having root authority.

One of the hottest topics when IT support first meets with development groups is the discussion of who will own “root” functionality. This generally starts out as a pleasant discussion with mutual respect among the participants. Development requests IT perform system administration functions while they keep root authority. IT responds that the only way to effectively perform system administration functions and to maintain integrity is for the data center to own “root.” This is the only way IT can maintain high reliability, availability, and serviceability (RAS) with their limited resources. Development then typically responds that they cannot effectively complete their jobs if they don’t have root authority. Many companies solve this dilemma by having joint root authority – data center owns it and several of the senior developers are also provided with root access. An internal support agreement is an excellent place to document such a root access. This model has proven to work well for many development organizations.

## **Roles and Responsibilities**

The following sections detail the various roles and responsibilities of IT personnel and support services typically included in the WCPA guide.

### **Internet Engineering**

Internet Engineering is the group responsible for operating the company’s Internet access. In a large company, it is typical to have multiple, geographically separate routes from internal networks to the Internet, both for load sharing and reliability. Internet Engineering is responsible for the principal external servers in the “demilitarized zone” or DMZ. The

DMZ is that portion of the network that sits behind the first firewall but outside of the main internal networks.

Typical responsibilities of Internet Engineering include:

- Determining requirements for Internet connectivity
- Contracting for ISP (Internet Service Provider) services
- Installing and maintaining external web, ftp, and e-mail servers
- Monitoring ISP performance and service level agreements

## Security Engineering

Security is a specialized enough topic that is called out separately in the WCPA. Typical responsibilities of Security Engineering include:

- Designing and maintaining firewall complex, possibly in conjunction with Internet Engineering
- Working with Internet Engineering to assure security of all external servers
- Working with Network Engineering to assure security of all internal networks
- Working with WebTone engineering to provide secure access through the firewall
- Designing and implementing methods for remote user authentication and data encryption

## Network Engineering

Typical responsibilities of **Network Engineering** include:

- Determining internal networking requirements, both for WAN's and LAN's
- Contracting with Telcos for WAN services
- Installing and maintaining all WAN and LAN routers, switches, and hubs
- Determining impact of new applications on the network

## Web Tone Engineering

Typical responsibilities of **WebTone Engineering** include:

- Working with Internet engineering to hand off incoming and outgoing web, ftp, and e-mail traffic

- Providing internal web server hosting
- Designing and maintaining a network of internal proxy cache servers at strategic points on the corporate Intranet

## Technical Services

Typical responsibilities of **Technical Services** include:

- Determining physical location of all server equipment
- Installing network connections and power
- Installing hardware, including third party equipment
- Conducting preventive maintenance diagnostics on all equipment
- Configuring operating system specific parameters
- Applying any operating system patches required
- Assisting database administration with DBMS installations
- Installing any unbundled 3<sup>rd</sup> party system management software
- Installing all required data center utilities
- Configuring and maintaining system security
- Monitoring system performance and capacity (CPU, memory, disk, network)
- Managing backup tape integrity and storage
- Providing on-call support, 7 x 24, or as specified
- Performing disaster recovery drills
- Establishing end-of-life plans to deactivate servers and applications
- Providing online availability statistics
- Providing system tuning for peak performance
- Performing capacity planning
- Establishing network connections to LAN and WAN, including ISP (Internet Service Provider) connections
- Providing and maintaining network databases
- Performing Security audits; monitoring security access
- Establishing user accounts and system (root) accounts
- Monitoring all daily processing
- Starting/restarting production jobs and applications
- Scheduling all online and batch processing
- Evaluating, developing, and implementing utilities and tools to support servers and applications in the production environment

## Hardware Support

Typical responsibilities of **Hardware Support** include:

- Supporting and resolving all hardware problems
- Handling all preventive maintenance within the data center for mission-critical servers

## Applications Support

Typical responsibilities of **Applications Support** include:

- Providing second-level application support as required
- Working with Technical Services and database administration to resolve complex application problems

## The WCPA Process

The WCPA process is synergistic, much in keeping with the web philosophy of shared resources. The various business units dictate what technologies and applications they want and need and entrust the data center to provide the technology and to reliably and securely support those applications.

It takes from one week to more than three months for an application to wind its way through the WCPA process, depending on its size and process for deployment. Working in Internet time, this is about half as long as the CSPA process for an equivalent client-server application. In shortening the production acceptance cycle, we have not cut corners, but rather found ways to use web technology to speed up the process. We begin the WCPA process by assigning a data center WCPA committee to work closely with the developers and users of a new application, preferably starting with its design stage. A WCPA web page is established for each project, serving as a focal point for communication during the entire process. The Table below provides a summary of typical WCPA implementation schedules.

**Sample WCPA Implementation Schedule**

Phase	Activity	Duration	% of WCPA Process
1	Information Gathering	1 week	10%
2	Resource Planning	2 weeks	20%
3	Implementation	6 weeks	50%
4	Production Cutover	2+ weeks	20%

If you are a user or a developer of an application requiring data center staff support, your first contact is Production Control. We assign a data center operations analyst to oversee the WCPA process and manage the WCPA committee.

This committee consists of Technical Services, Database Administration, Security Engineering, WebTone Engineering, Internet Engineering, Production Control, and Computer Operations personnel from the data center, along with the application's project leader.

The team collaborates to foster the application all the way through the alpha, beta, and pre-production stages. Once an application is finally ready for production use, the data center infrastructure takes charge of its implementation and security. Technical Services, controls Root access to the application regardless of where the application's server is located, and all changes must follow the change control process.

Preparing an application for production happens in four phases:

- **Phase I:** Information gathering
- **Phase II:** Resource planning time
- **Phase III:** Implementation period
- **Phase IV:** Application and Data Center Services are tested online for an undetermined time

**Phase I** is the information-gathering phase. Phase I takes about a week to initially complete, and then continues as needed throughout the WCPA. During the initial phase, the user will contact Production Control and fill out the online WCPA questionnaire available on the Production Control web page. This questionnaire contains general information about the project, including its name, the names of its development group, owner and leader, a description of the application, whether it needs a database, what type of hardware it will use, whether it requires continuous (7 x 24) support, where users are production freeze, software distribution, WCPA questionnaire sign-off, and a production implementation date.

**Phase II** is resource-planning time. The Production Control Operations Analyst assigned to the project reviews the questionnaire and, based on the application's needs, formulates an appropriate WCPA committee and works with Technical Services to define data center space, equipment, personnel allocations, and costs to support the project. The Operations Analyst also works on the WCPA questionnaire with the application's project leader. The project leader orders needed equipment with the recommendation from Technical Services. This is where the Production Guide, which includes the services provided by the Data Center, the Personalized Communications, and the Internal Support Agreement come into place. Here it's important to communicate the services provided, set expectations, and, more importantly, communicate the services not provided.

**Phase III** is the implementation period. It usually takes one month to complete, depending on the size and complexity of the application. Technical Services personnel install the necessary hardware, software, and all supporting utilities on the server. The data center's Database Administration people work with the application developers to prepare the supporting database (if needed), and then relay disk partition information and database creation scripts for installation and execution by Technical Services. Applications Development installs the application and performs testing.

Finally, in **Phase IV**, the application and all data center support services are brought online and tested for as long as it takes to ensure the application can run reliably in a production environment. Also, during this final phase, the Operations Analyst adds the application to automated systems that track server and application availability worldwide.



Once fully completed, an application's WCPA questionnaire, hardware, and software are maintained by the data center. Database Administration maintains and upgrades the database and software, making any needed system changes such as adding dumps devices, increasing database sizes, and analyzing and reconciling maintenance errors. Production Control manages job scheduling, restarts applications, and makes network support file changes, as necessary. Technical Services maintains the operating system software and hardware, formats and repartitions disks, installs unbundled software, and maintains and configures system security and network services. Once the application is ready for production, the committee approves the WCPA for sign-off. It now becomes a working service-level agreement for supporting the application in production. Any deviations must go through the Change Control process.

## **What IT Should/Should Not Support**

In deploying web-centric applications, it is often more important for IT to know what services you don't provide, particularly in those gray areas where previous practices might lead to differences of opinion unless support policies are clear. For instance, in a traditional client-server environment, IT controlled not only all servers, but also all desktops where client software was installed. All application software can be downloaded at run time. In such a scenario, especially if the application is deployed over the Internet, IT may have no control of client desktops, other than to specify a minimal browser revision level. If a business unit uses some special, non-IT supported browser and the application runs into difficulty, IT might do an initial diagnosis but normally should pass along the problem to the business unit, who chose the unsupported browser in the first place.

Besides caveats, there are a variety of responsibilities IT and business unit customers accept as part of the Internal Support Agreement. Customers are responsible for providing the list of services they need to support their operations. The levels of service should be held to as few categories as necessary. Customers are expected to work closely with IT to ensure all users carefully select, control, and regularly change user passwords, according to corporate security policy. Final configurations are the responsibility of IT, implemented and supported as defined by the WCPA questionnaire. In cooperation with the local facilities organization, any distributed web and proxy servers are managed to ensure an adequate environment for systems. The Internal Support Agreement also spells out what some consider the ultimate responsibility: funding. The business units, not IT, should be responsible for obtaining funding and approval for all their appropriate capital assets to ensure sufficient computing resources. They are responsible for future adds, moves, and changes, as well as funding for those future systems. If management doesn't allocate money and resources to meet those customer needs, IT and the customer must and will negotiate a reduced level of support.

Finally, anything included in the service-level agreement and budgeted for IT services, will be provide by IT. Anything not included is either done without or later negotiated.

The WCPA is not foolproof. In fact, there are many ways to defeat its purpose:

- Put an application into production without thorough testing and documentation
- Treat every application as an exception and take shortcuts
- Reassign application developers to new projects before completing deployment of the current application
- Be too busy to thoroughly document
- Let the WCPA gather dust, versus making it an ongoing process

Barring such willful ignorance or neglect, the WCPA doesn't just happen on its own. As an organization there are some things you can do to make sure the WCPA succeeds in your organization:

- Start early; don't wait until an application is nearly ready for production
- Intimately involve developers and users; build their sense of ownership
- Always adhere, without exception, to the WCPA for new applications and releases
- Clearly spell out and document responsibilities and duties in the WCPA questionnaire.