

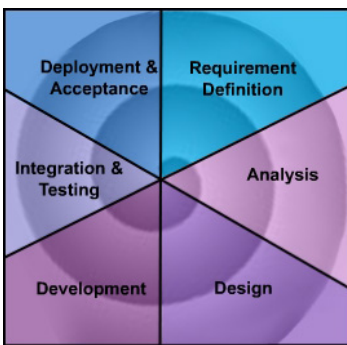
The Bottom Line

TECHNOLOGY SOLUTIONS FOR SMALL AND MID-SIZED COMPANIES

Volume 4, Issue 2

February 2007

Getting the most out of your software development project



Software development is challenged with late delivery, budget overruns, and project changes. Many business owners that tried to have an application developed will tell you that the result was not what they anticipated. What do you do when you need a system created or customized for your business?

1. Hire a competent firm and check their credentials. Is the "company" just a person doing work on the side from his other day job? If yes, find someone else. This is one time when hiring a professional really pays. How will the firm make sure they know what you want? – Listen for the words scope, requirements, "wireframes", implementation plan, etc.

Has the company developed a similar system or one of similar size to the one you need? What do they plan to give you during the course of the project? – There should be plenty of opportunity for you to see and understand what is being developed. Are they willing to give you references?

2. Be involved. Plan to provide a lot of input to the project. Your developer wants to create the right features and functions but he cannot know your business as well as you.
3. Identify the tasks that you want the software to accomplish. It's easiest to think about each person that will use the program and identify what functions they will need the system to perform.
4. Identify any specific requirements/needs that relate to the tasks you've identified.
5. Make sure you understand and account for ongoing maintenance of the system being

developed.

6. Changes happen. It is nearly impossible to identify everything up-front. The developer should document changes and identify the impact to scope, time, and project budget. Remember that the later in the process you request a change, the more it will cost.
7. Test. Test. Test. Expect to find some bugs and then retest everything after the developer makes corrections. The developer does test the system, but you test it as an end-user and might identify something that a developer might not perceive as a problem.
8. Plan time for rollout and training. Change is hard – depending on the system, you might want to rollout in phases. Consider training some employees and having them train the remaining personnel. This promotes buy-in to the process and creates "super-users" to act as mentors after the development team is gone.

Company News:

Jankovsky speaks at the 2007 IPRA/IAPG Conference

Jody Jankovsky, Managing Partner and Owner of Black | Line Consulting, was a guest speaker at the 2007 Illinois Parks and Recreation Conference held January 25-27, 2007, in Chicago. His seminar, entitled, "Business Continuity-Going beyond "Disaster Recovery", discussed what Business Continuity Planning (BCP) is, what it is not, and why you should do it.

The term "Business Continuity" replaces the older expression "Disaster Recovery" as the term that best describes the planning needed to address interruptions to a business. Disasters are a piece of the BCP but only represent fraction of scenarios that can interrupt a business.

Business Continuity does not focus exclusively on information technology (IT) components but takes a more holistic approach to the entire organization. It includes the IT functions but also addresses the impact and reaction by non-IT areas of the organization. IT infrastructure supports the operations of the organization so interruptions will affect the organization's general well-being. However, if the BCP focuses only on IT, critical business processes are left without a safety net.

The more an organization relies on technology to operate, the more important it is to address business continuity. Downed systems represent significant financial risk and affect how an organization is perceived by those externally. The BCP addresses risk management by assessing the various levels of risk to an organization and prioritizing each point of failure based on the organization's need.

For more information on BCP, download the presentation at www.blacklineconsulting.com.

The Bottom Line

TECHNOLOGY SOLUTIONS FOR SMALL AND MID-SIZED COMPANIES

Black | Line Consulting
1560 Wall Street
Suite 105
Naperville, IL 60563
Phone: 630-388-1700
Fax: 630-388-1697
E-mail: sales@blacklineconsulting.com

PRESORT STANDARD
U.S. POSTAGE
PAID
PERMIT NO. 486
NAPERVILLE, IL

Getting the most out of your software development project

Tips and Techniques: How secure is your password?

Tips and Techniques: How secure is your password?

People forget passwords. It's just one of those things that computer support personnel deal with on a daily basis. To help them remember, users often use simple things like their child's first name and birth date, their dog's name, or their street address. They use just about anything that reminds them of their password.

Using such simple passwords is just like locking your front door and leaving the key under the mat. A hacker doesn't even have to use specialized tools to obtain basic information about you. He can gather your personal information and try different combinations as potential passwords.

What can you do to help ensure your systems are secure?

1. Create password policies that enforce:
 - A. Password History – Ensures that a user cannot re-use a password within the specified number of passwords stored in the history. For example, if set to five, the user would



have to reset the password five times before the system would allow the reuse of the first password.

B. Minimum Password Age – Establishes a minimum number of days that must pass before the password the user can change the password again; generally a minimum of three days.

C. Maximum Password Age – Used to force users to change their passwords on a regular basis.

D. Password Complexity Requirements – Forces users to incorporate different elements into their passwords, making them harder to crack. For example: i. Do not allow passwords that contain significant portions of a user's name or user ID, ii. Enforce a minimum password length, usually at least seven or eight characters, and iii. require passwords to contain characters from at least three of the following character sets: uppercase characters (A-Z), lowercase characters (a-z), numbers (0-9), and special characters (&, \$, #, or %, etc.)

2. Teach your employees how to create easy to remember secure passwords that comply with the password complexity requirements you define.
3. Require the use of a different password for each major system you need to secure.