



## CrownPeak Technology

### **Risk in Content Management Implementations: Examining Software Services | Business Whitepaper**

CrownPeak  
5880 W. Jefferson Blvd  
Unit G  
Los Angeles, CA 90016

[sales@crowpeak.com](mailto:sales@crowpeak.com)  
[www.crowpeak.com](http://www.crowpeak.com)  
Toll Free: 866-877-5858  
Tel: 310-841-5920

## Risk

Everything we endeavor to accomplish has risk associated with it. The relationship between risk and reward is a factor in virtually every decision we make – every decision we make rationally, that is. Of course, other factors enter into decisions: cost, time constraints, emotions (pride, for example), and so on. But risk is omnipresent.

In a perfect world, where full information is available about every decision and the outcome of each decision is clear, risk would not exist. For game theorists, gamblers, and business people, that would be a dull world indeed. But because risk in the real world exists in abundance, those who can best analyze the risk/return equation are often the most successful – be they gamblers, economists, or businesspeople.

In the world of content management, the reality of the risk equation is clear. Many large organizations have paid high fees to enable inflexible and esoteric applications. Mid-size companies have suffered with custom-built solutions that actually prevent them from managing online content readily. Others have opted for the risk of inaction, and have paid with poorly presented and managed online content – to the detriment of their brand and their customer relationships. Often, inaction costs more than action, with highly paid programmers coding pages manually, or maintaining monolithic custom-built applications.

Still, success isn't entirely foreign. The landscape of Web content management solutions has changed dramatically in the last few years. Products have matured and new entrants have offered customers new choices. Some organizations, indeed, have figured out what it takes to succeed at managing content (and everything that goes along with it). There's a much greater congruence between cost and value. Companies manage their Web properties with more power, flexibility and ease than ever before. The application they have chosen saves the organization money and increases shareholder value. And in succeeding, they have learned something about risk.

Indeed, some of these success stories have sprung from organizations that have not only taken advantage of the benefits of a Web content management system but have lessened their risk by outsourcing their content management system altogether. In the right situation, outsourcing – especially outsourcing to a specialized Software Service provider can be a good option.

## Risk in Content Management

Various risk factors are inherent in deploying a content management solution; let's consider each in turn:

### Risk of data loss

A content management system (CMS) does not replace site backup. A live Web site normally incorporates elements and functionality that don't come from the CMS – search, BBS, advertisements, user management systems, etc. Reliable Web serving requires a full backup process for the Web site and a redundant server environment. When the Website fails, the CMS can often re-publish the content, but it can't re-publish functional elements like search.

Likewise, the content management system needs to be backed-up, and a redundant instance of the CMS on separate hardware is a good investment if your content update process is mission critical. Backing up data from the content management system is the other essential requirement. It's mandatory to store those backups offsite, and have in place a recovery plan for both the data and the CMS.

Implemented well, a CMS can in fact minimize the risk of data loss, but it does so at a price. Redundant environments can double or more than double out-of-pocket costs. That rule is inviolate; the level of risk of data loss in a traditional IT environment is directly related to the size of the investment – the more you spend, the lower the risk.

### Risk of a security breach

Organizations worry about security on a content management system for one of two reasons. First, does the system house high-security data, which needs to be protected from being stolen and possibly distributed? This matters most to healthcare, government, financial services and law firms, but applies to any type of organization with sensitive data. Second, could malicious intruders delete or modify content? We've already seen too many examples of hackers breaking into sites to post phony data or attempt to manipulate stock prices.

Security for a CMS is a crucial, and sizeable, topic by itself. It's entirely possible to manage security associated with the CMS server and its software components, the network environment, the physical environment, and the application itself – and still lose. The most common security breach has to do with passwords being given out to hackers through carelessness or gullibility.

Assuming that the physical environment is in a highly secure data center and your staff doesn't expose passwords to the wrong people, security management of the network, the application and CMS server environment are still 24/7/365 jobs. If monitoring isn't set up (or no one is home to do the monitoring), it will be impossible for anyone to know you've been hacked until you come in on Monday and your data is gone, or your site is a scandal – or worse, you've been hacked but you don't find out until you make the papers. If nobody is patching the OS and software to close openings to hackers, you will quickly become a target. Like backups and redundancy, the more time and money you invest on security, the lower your risk exposure.

### Risk of cost/timing overruns, spiraling costs

The cost of implementing and maintaining a content management system can be hard to estimate and even harder to control. Everyone is familiar with the four-month, \$250,000 project that morphed into the 14-month, \$1.2 million project. Internally managed projects often have unmonitored costs for IT staff. Managing project budgets carefully, selecting strong implementation partners, and implementing quickly to avoid "moving target requirements" can all help to mitigate project overrun risk.

Managing the application also has a cost associated with it, but the most commonly underestimated cost involves adjusting and modifying the CMS itself. Web sites change, processes change, and new Web sites appear. A good CMS implementation needs to evolve in concert with the organization and organizational requirements. This can, however, be the easiest element of cost to underestimate. The risk in not budgeting for application evolution is that the application can become a barrier to making changes to the Web site. This translates to inefficiencies driven by the application that was intended to make you more efficient – a sad state of affairs.

## Risk of implementation failure – system doesn't meet requirements or doesn't work well – or at all

Application failure can be a difficult thing to judge. Is an application a failure if it solves one problem very well, but doesn't solve two other problems that weren't apparent when the implementation was planned? Is an application a failure if it irritates the people who use it? Or if only a few of the intended users ever bother to adopt it?

The answer to all of these questions is probably "yes." That said, these are all common outcomes with CMS systems. We've also seen CMS systems purchased and never used, or more troubling, CMS projects cancelled after a large cost overrun.

Mitigating the risk of implementation failure in CMS projects is similar to risk mitigation for any IT project. Clear goals, dedicated and experienced teams, and quick project lifecycles all help. Once the project is complete, assigning responsibility for managing application usability and extension is the key to having a CMS that works as well (or better) on the 360th day as it did when it was launched – and mitigating the risk of non-adoption. Not budgeting and planning for application evolution is a very good way to shorten the time to application failure and application non-adoption.

## The risk of doing nothing

The risk of inaction is worth considering. In a recent anecdote, we received a note from an IT manager in a mid-size public corporation saying that he had solved his company's content management problem by adding to his staff and re-writing a custom application from scratch. In addition to himself, he had four programmers, two HTML developers and a QA person, all dedicated to the problem – all for a 500-page Web site. Of course, he wasn't calculating the cost of his group when evaluating other solutions, but in this case, the solution to throw staff at the problem was clearly a poor bet.

As Canadian power rock trio Rush said in their song *Freewill*, "If you choose not to decide, you still have made a choice." The mid-level IT manager who was probably spending a million dollars annually to manage a 500-page Web site is a living testament to the wisdom of Rush's analysis.

The decision to maintain an internal process was almost certainly not evaluated as a "build or buy" decision. In fact, there was probably never an actual decision on content management made in this case. Perhaps that ought to be called "the risk of not evaluating the issue."

## Outsourcing – Software as a Service

Hosted content management applications, like other hosted business applications, aren't appropriate in every instance. Where the data is not available over the public network (as with highly secure financial or personal information), or where the CMS is tightly integrated with back-office applications like an ERP system that might be drawing real-time inventory data for a client extranet, an outsourced CMS is probably not the answer.

But as mid-market Web site content management systems provide simpler and less costly solutions for the great majority of Web content management requirements, so too can the hosted application provide for additional benefits – and, big surprise – lower risk.

There is a significant difference between the two types of outsourced solutions: outsourcing a traditional application to an ASP or an outsourcing vendor, who will host and manage it for you,

and outsourcing to a Software as a Service (SaaS) vendor, which manages its own, highly-specific application. Among the latter are CrownPeak Technology, WebSideStory, and Clickability; more traditional outsourcing providers include IBM, EDS, and Accenture.

In summary, the difference between the two is that outsourcing vendors provide many different types of applications and even manage those applications on-site, where Software as a Service companies concentrate on a specific application or application type, available solely as a Web application. Software as a Service vendors typically deliver at a much lower cost because they provide a single application to many customers. For the balance of this article, we will concentrate on the Software as a Service CMS option.

## Risk of an Installed CMS vs. Risk from CMS Software as a Service

### Risk Of Cost/Time Overruns

Typically, a hosted application can take advantage of providing a singular software, hardware, network, management and support solution across a large number of clients. Such shared costs across multiple clients means that SaaS CMS solutions are often 30 to 50 percent less expensive than their installed counterparts.

Additionally, a good hosted CMS will provide rapid implementation and customization services and will often build these costs into the monthly fee. Because SaaS vendors work with only one application, they typically provide fixed bids for implementation and customization work, good warranties on that work, and ongoing support to “tweak” the project. The key is the nature of the contract. Installed vendors also provide excellent warranties and fixed bid contracts. Compare the service elements included in fees carefully. Also compare ongoing support contracts – some installed vendors provide service contracts comparable to SaaS vendor’s Service Level Agreement (SLA).

### Risk of Data Loss

An outsourced content management system will normally minimize risk for data loss because it is a separate system, managed by a different group in a different environment, with separate (and therefore redundant) backup and recovery procedures. These benefits are also typically delivered at a lower cost than any backup and recovery process for an insourced solution because data backup and recovery are a normal part of SaaS operations, and the costs are spread across many clients. Additionally, SaaS vendors are only managing one application, and so can afford to have very high-level procedures for backup and recovery.

The question becomes, “how valuable are our data and what are the minimum steps we need to take to ensure that we don’t lose it.” It may be that the SaaS vendor is actually spending (and costing) too much money – even spread across many clients – for data backup and recovery. This is especially true when working with large, redundant data sets.

### Risk of a Security Breach

As with data loss, an outsourced content management system can decrease the risk of a security breach in an organization’s Web site, for the same reasons – SaaS vendors manage only one application, but spread the costs across many clients. The consequences of a security breach could be catastrophic for a CMS-as-service vendor. That’s the reason for the extra

energy directed at security operations for the application. Most SaaS vendors have full-time dedicated staff working on security 24/7/365. The recent SQL Worm, for example, hit none of the Content Management SaaS vendors but how many Microsoft Content Server implementations were affected? It's simply a matter of attention. The more effort involved, the better the results. Compare the program from the SaaS vendor to the alternative.

## Risk of Implementation Failure

Because customers are paying on a monthly basis, the outsourced content management company has a great incentive to make sure end-users are happy. That by no means guarantees that the application will work better or that customer service will perform better, but it should be a good indication. The better SaaS firms have programs to continually poll system users for satisfaction and suggestions. Every software company is constantly tweaking the product to roll out new features and functions that benefit the client, but the SaaS vendor has the advantage of product changes taking effect immediately. Put simply, if the SaaS vendor doesn't provide a satisfactory application, the next step is easy: terminate the contract. The option to terminate mitigates the financial risk element, but starting all over again clearly represents failure.

The real measure for risk in implementation failure is adoption. If the users of the system believe in the project, and take an active interest in getting the application to work the way they'd like, they will use it. If the roll-out process is smooth and the training is exciting and empowering, users will adopt. If users feel that they have the ability to request changes and have good access to support, they will remain users. Most products on the market have good features and reasonably good user interfaces. In the end, the most critical project element is managing an effective rollout process.

## Risk of Doing Something

Comparing the risk of the status quo against the risk of doing something that doesn't provide a good return, the equation becomes less complex when the risk of implementation failure and the cost of the application are low. The best way to keep these risks low is to operate simply. Pick workgroup projects and run a fast implementation using rapid prototyping techniques. Pick a product that stresses ease of implementation and ease of management. List the primary business benefits of the project, and then pick a product or service that meets 80 percent of those needs. Review the project 120 days after completion to ensure that you have met business needs and addressed user adoption.

## A Final Word

The concept of Enterprise Content Management has been around for about five years now, driven by the early players in the game. Even so, most content management projects are delivered to discreet workgroups that are publishing specific sets of content. In many cases, the value of having an enterprise implementation is debatable. Remember that as project size and complexity increase, so do each of the risk elements listed above. Emphasizing speed of implementation – which is closely tied to speed and ease of system management and evolution – and stressing workgroup-sized implementations for workgroup-size projects is the low-risk future of the content management business.