

# The e-Business Audit

Once a company builds its e-Business that e-Business needs to be continually audited.

Why do e-Businesses need to be audited? Take a look at table 1. There's a lot of issues - and possible liability - there. From the hacker who changes your website to employees who surf for porn. From customer service agents who provide anything but to e-Commerce sites that take orders for nonexistent merchandise. I like to call this eBusiness Health<sup>tm</sup>.

<b>Response time/availability</b>
<b>Accessibility</b>
<b>Ergonomics</b>
<b>Logistics</b>
<b>Customer service</b>
<b>Security (passwords, penetration, intrusion)</b>
<b>Privacy</b>
<b>Navigability</b>
<b>Fulfillment</b>
<b>Liability</b>
<b>Copyright infringement</b>
<b>Employee, illegal usage, porn</b>
<b>Search engine coverage</b>

Table 1. A sampling of the components of e-Business Health.

This paper will provide an annotated checklist approach to auditing your e-Business.

## **Organizing Your e-Business Audit**

While it is recommended that you hire an external consulting firm to perform this critical effort your EDP audit department , with adequate training, would be a sufficient alternative.

The reason why I much prefer an external auditor is that a "neutral, third party" is usually more objective since they are not stakeholders nor are they friendly with stakeholders. There's nothing like an unbiased opinion.

At a minimum the auditor should obtain the following documentation:

1. **A diagram of the application system:** An e-Business system is not unlike any other computer system. It has processes (e.g. process credit card) and entities (e.g. airline ticket) and shows the flow of data between the entities via the processes. Figure 1 shows a typical data flow diagram at its highest, or conceptual, level.

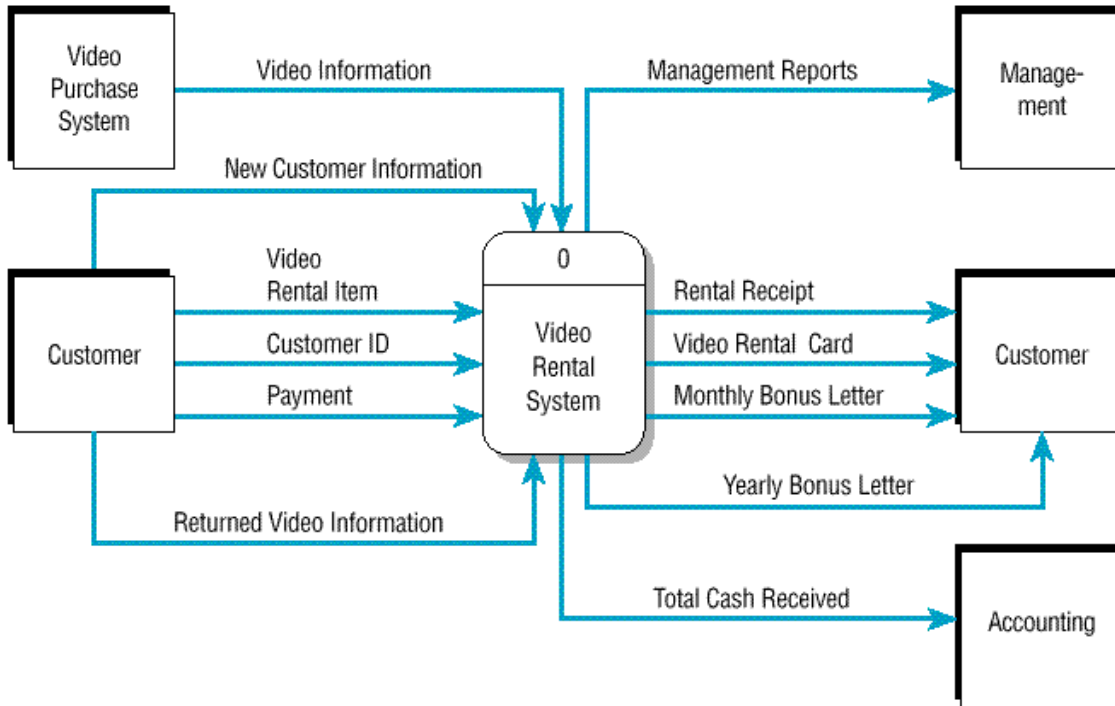


Figure 1. A data flow diagram for a video rental system.

2. **A network diagram:** Most modern computer systems are developed using one of several traditional network architectures (i.e. two-tier, three-tier, etc.). Add EDI and/or Internet connectivity and you have quite a sophisticated environment. The auditor will need a roadmap to this environment to be able to determine if there are any connectivity issues. Figure 2 demonstrates what a simple network diagram should look like.

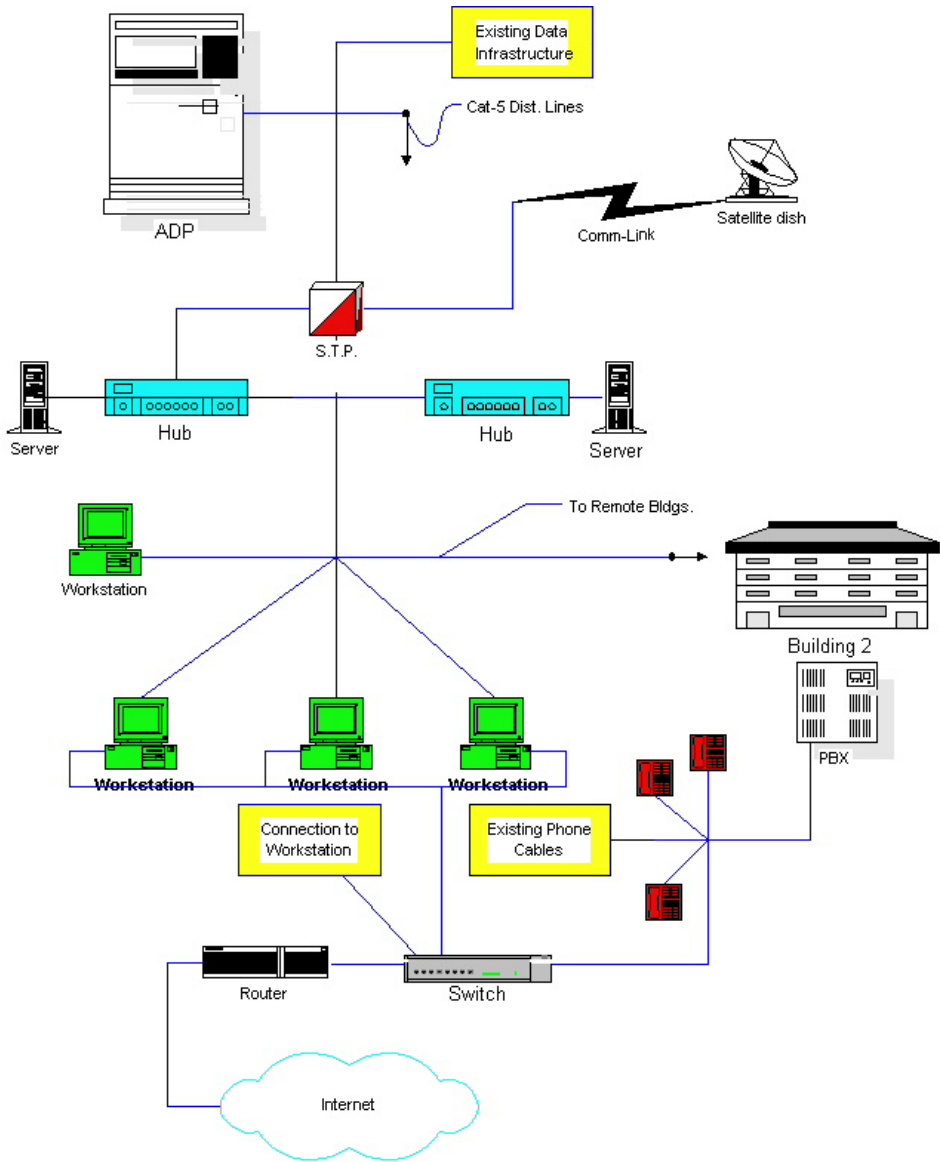


Figure 2. A typical network diagram.

3. **Staff hierarchy diagram.** A complete list, preferably a diagram that shows direct reports, along with phone numbers and/or e-mail addresses is required.

One would think that a modern organization would have these three items readily available. Think again. In my own experience, few of the organizations that I audit possess all three of these required items. Few possess even two.

If these are not available to the auditor, my recommendation is start the audit effort with a series of brainstorming sessions where, at least, the two

diagrams are created. Even if diagrams are available one or more brainstorming sessions are still advisable. This provides the auditors a "walk through" where system and network architects can be questioned directly. This invariably speeds up the audit process.

Once the preliminary way has been completed (i.e. understanding the system), the auditor can proceed to go through his or her paces in a logical methodical manner. The following sections, presented as a series of checklist, represents areas of the audit that can actually be performed in any order.

The checklist is actually a series of questions or areas to be studied. The responses to these questions form the data collected for input to the final Audit report. The final Audit report on a company's e-Business Health will contain problems found, issues overlooked as well as recommendations for improvement.

For example, the auditor might find that the company has done inadequate security testing. The recommendation here might be to bring in a "white hat" to perform both penetration as well as intrusion testing. Alternatively, the audit might uncover a deficiency in the fulfillment processes the company follows to ship products purchased to the customer. Again, the Audit report will make recommendations for improvement.

Let's begin at the beginning.

## **1.0 Systemic Audit**

It's surprising that many companies spend millions on dollars on advertising budgets to draw more "eyeballs" to their sites but never factor in whether or not the projected additional load can be supported by the current system configuration.

A systemic audit looks at such things as response time, network architecture and linkages.

1.1 Response time. Measurables in this section include actual response time versus projected response time. In spite of the advances in supplying high-bandwidth connections to consumers, the vast majority of PCs are connected to the Web with little more than a 56Kb modem and good intentions. This means that sites that are highly graphical or use add-ons such as Macromedia Flash will appear slow to download.

Given the wide variety of modem-types auditors should test the response time of the site using different scenarios such as:

- Using a DSL or cable modem connection
- Using a 56kb connection
- Using a 28Kb connection
- At random times during the day, particularly 9 a.m (start of work day) and 4 p.m. (kids home from school)

Web sites such as netmechanic.com, a subscription service, can assist in this endeavor by checking for slow response time directly from their Web sites.

1.2 Broken links: One of the top five irritants that web surfers report is clicking on a link and getting a "nonexistent page" error message. This is often the result of system maintenance where web programmers move the actual page but neglect to modify the link to that page. Unfortunately, this is a frequent occurrence. One of a number of tools, including netmechanic.com, can assist in tracking down these broken links.

1.3 Database audit. Originally the web was a simple place. It consisted of mostly text and there was nary a database in sight. Today, the web is filled to the brim with databases. The addition of databases makes the audit process even more complex. Since programming code is used to query, and perhaps even

calculate, against that database it is imperative that random checks be performed in an effort to pinpoint database query and calculation errors.

Essentially, auditing database access is similar to the traditional IT (information technology) QA (quality assurance) process. One or more scripts must be written which will take that database through its paces. For example, if a database program calculates insurance rates based on a zip code then that calculation should be duplicated either manually or in a different parallel automated fashion to ensure that the result is correct.

The same can be said for information that visitors to the site enter via a form. Is the information being entered the same that is being sent to the database?

1.4 Network audit. The network itself, including node servers, should be tested to see if it is effectively configured to provide optimum response. It is not uncommon to find the Web development group separated from the traditional IT development group. This means that one frequently finds network configurations architected inappropriately for the task at hand. For example, a site attracting tens of thousands of hits a day would do well to run a multitude of web servers rather than just one.

Most organizations use one or more ISPs (Internet Service Providers) to host their sites. The auditor should carefully gauge the level of service provided by these ISPs as well.

## **2.0 Security and Quality**

There is no one topic that is discussed more in the press than Internet security. From "love bug" viruses to wily hackers breaking into Western Union, security is an important component of the e-Business audit.

It is worthwhile to keep in mind that the auditor is not a security auditor, nor should he be. His or her role is to do a top level assessment of the security of

the e-Business and, if warranted, recommend the services a security firm well-versed in penetration and intrusion testing.

The entire issue of security is wrapped up within the more comprehensive issue of quality. This section will address both issues.

2.1 Review the security plan. All organizations must possess a security plan - in writing. If they do not have this then they are severely deficient. The plan, at a minimum, should address:

2.1.1 Authentication. Is the person who he or she says he is.

2.1.2 Authorization. What users have what privileges. In other words "who can do what?".

2.1.3 Information integrity. Can the end-user maliciously modify the information?

2.1.4 Detection. Once a problem is identified how is it handled.

2.2 Passwords. Passwords are the first shield of protection against malicious attacks upon your e-Business. Questions to ask in this section include:

2.2.1 Is anonymous login permitted? Under what conditions.

2.2.2 Is a password scanner periodically used to determine if passwords used can be hacked? Examples of this sort of utility include L0phtcrack.com for NT and [www.users.dircon.co.uk/~crypto](http://www.users.dircon.co.uk/~crypto) for Unix.

2.2.3 How often are passwords changed?

2.2.4 How often are administrative accounts used to logon to systems? Passwords are hard to remember. This means that, in order to quickly gain entrance to systems, administrative and programming systems people often create easy-to-remember passwords such as admin. These are the first passwords that hackers try to gain entrance into a system.

2.3 Staff background. Administrative network staff must have a security background as well as a technical background. Those wishing to train their staffs would do well to look into the Security Skills Certification Program provided by [www.sans.org](http://www.sans.org).

2.4 Connectivity. Today's organization may have many external connections (i.e. partners, EDI, etc.). For each company connected to, the auditor should examine:

2.4.1 The data being passed between organizations. Is what the company sent being received correctly?

2.4.2 The security of the connection. How is the data being transmitted? Is it required to be secure? Is encryption being used?

2.4.3 If encryption is indeed being used, it must be determined whether an appropriate algorithm is being deployed.

2.5 The product base. All organizations invest and then use a great deal of third-party software. As publicized by the press much of this software, particularly browsers and e-mail packages but word processing packages as well, contain security holes that, left unpatched, put the organization at risk. Therefore, for each software package (for Net purposes) being used:

2.5.1 Check for publicized security holes.

2.5.2 Check for availability of software patches. Always upgrade to the latest version of software and apply the latest patches.

2.5.3 Check to see if patches have been successfully applied.

2.5.4 Check security software for security holes. Security software, such as your firewall, can contain security holes just like any other type of software. Check for updates.

2.6 In-house development. The vast majority of e-Business software is written by in-house programming staff. When writing for the Web it is important to ensure that your own staff doesn't leave gapping holes through which

malicious outsiders can gain entrance. There are a variety of programming "loopholes", so to speak, that open the door wide to hackers:

2.6.1. In programming parlance a "GET" sends data from the browser (client) to the server. For example, look at the query string below:

```
http://www.site.com/process_card.asp?cardnumber=123456789
```

All HTTP (hypertext transport protocol) requests get logged into the server log as straight text as shown below:

```
2000-09-15 00:12:30 - W3SVC1 GET/process_card.asp  
cardnumber=123456789 200 0 623 360 570  
80 HTTP/1.1 Mozilla/4.0+(compatible;+5.01;+Windows+NT)
```

Not only is the credit card number clearly visible in the log but it might also be stored in the browser's history file exposing this sensitive information to someone else using the same machine later on.

Security organizations recommend the utilization of the POST method rather than the GET method for this reason.

2.6.2 Are the programmers using "hidden" fields to pass sensitive information? An example of this is relying on hidden form fields used with shopping carts. The hidden fields are sometimes used to send the item price when the customer submits the form. It is rather easy for a malicious user to save the web page to his or her own PC, change the hidden field to reflect any price he or she wants and then submit it.

2.6.3 One way to combat the problem discussed in 2.6.2 is to use a hash methodology. A hash is a function that processes a variable

length-input and produces a fixed-length output. Since it is difficult to reverse the process the sensitive data transmitted in this matter is secured. The auditor is required to assess the utilization of this methodology given any problems he or she might find in assessing 2.6.2.

#### 2.6.4 Is sensitive data being stored in ASP or JSP pages?

Microsoft's Internet Information Server (IIS) contains a number of security flaws that, under certain circumstances, allows the source of an ASP or JSP page to be displayed rather than executed. In other words, the source code is visible to anyone browsing that particular web site. If sensitive data, such as passwords, are being stored in the code than this sensitive data will be displayed as well. The rule here is to not hardcode any security credentials into the page itself.

2.6.5 Are application-specific accounts with rights identified early in the development cycle? There are two types of security. One is referred to as "declarative" and takes place when access control is set from outset the application program. "Programmatic" security occurs when the program itself checks the rights of the person accessing the system. When developing code for the e-Business it is imperative that the rights issued be addressed early on in the development cycle. Questions to ask include:

- How many groups will be accessing the data?
- Will each group have the same rights?
- Will you need to distinguish between different users within a group?
- Will some pages permit anonymous access while others enforce authentication?

2.6.6 How are you dealing with cross-site scripting? When sites accept user-provided data (e.g. registration information, bulletin boards), which is then used to build dynamic pages (i.e. pages created on the spur of the moment) the potential for security problems are increased a hundred-fold. No longer is the web content created entirely by the web designers - some of it now comes from other users. The risk comes from the existence of a number of ways in which text can be entered to simulate code. This code can then be executed as any other code written by the web designers - except that it was written by a malicious user instead.

Both JavaScript and html can be manipulated to contain malicious code. The malicious code can perform a number of activities such as redirecting users to other sites, modifying cookies, etc. More information on this topic can be obtained from CERT's website at <http://www.cert.org/advisories/CA-2000-02.html> and [http://www.cert.org/tech\\_tips/malicious\\_code\\_mitigation.html](http://www.cert.org/tech_tips/malicious_code_mitigation.html).

2.6.7 Have you checked wizard-generated/sample code? Often programmers "re-use" sample code they find on the Web or make use of generated code from web development tools. Often the sample or generated code contains hardcoded credentials to access databases, directories, etc. The auditor will want to make sure that this is not the case in the code being audited.

2.6.8 Are code reviews being performed? There is nothing worse than the lone programmer. Many of the problems discussed in the sections above can be negated if the code all programmers write is subject to a peer review. Code reviews, a mainstay of traditional quality-oriented programming methodology, are rarely done in today's fast-paced e-Business environment. This is one of the reasons why there are so many security break-ins.

2.6.9 Web server review. In order to run programs on the Web. Many organizations use the CGI (common gateway interface) to enable programs (i.e. scripts) to run on their servers. CGI is not only a gateway for your programming code (i.e. via data collections forms). It is also a gateway for hackers to gain access to your systems. Vulnerable CGI programs present an attractive target to intruders because they are easy to locate, and usually operate with the privileges and power of the web server software itself. The replacement of Janet Reno's picture with that of Hitler on the Department of Justice web site is an example of just this sort of CGI hole. The following questions must be asked of developers using CGI:

- Are CGI interpreters located in bin directories? This should not be the case because you are providing the hacker with all the capabilities he or she needs to insert malicious code and then run it directly from your server.
- Is CGI support configured when not needed?
- Are you using remote Procedure Calls (RPC)? Remote Procedure Calls allow programs on one computer to execute programs on a second computer. There is much evidence that the majority of distributed denial of service attacks launched during 1999 and early 2000 were executed by systems that had RPC vulnerabilities. It is recommended that, wherever possible, turn off and/or remove these services on machines directly accessible from the Internet. If this is not possible that at least ensure that the latest patches to the software are installed since these mitigate some of the known security holes.
- Is IIS (Internet Information Server) being used? This is the software used on most web sites deployed on Windows NT and Windows 2000 servers. Programming flaws in IIS's Remote

Data Services (RDS) are being used by hackers to run remote commands with administrator privileges. Microsoft's own web site discusses methodologies to use to combat these flaws.

2.7 Testing. Pre-PC testing was a slow and meticulous process. Today's faster pace means that inadequate testing is being performed by most organizations. In addition, many organizations forego security testing entirely. In this section of the audit we determine whether adequate security is being performed.

2.7.1 Has penetration testing been done? Penetration testing is used to assess the type and extent of security-related vulnerabilities in systems and networks, testing network security perimeters, and empirically verifying the resistance of applications to misuse and exploitation. While it is possible that system administrators are sophisticated enough to be able to utilize the toolsets available to scan the systems for vulnerabilities, a whole host of "white hat" hacker security consulting firms has sprung up over the past several years and it is these folks that are recommended.

2.7.2 Has intrusion testing been done? There are a whole host of software tools available on the market today that "monitor" systems and report on possible intrusions. These are referred to as Intrusion Detection Systems (IDS). In this section of the audit we determine whether an IDS is being used and how effectively it is used.

2.7.3 Is there a QA (quality assurance) function? While QA departments have been a traditional part of the IT function for decades, many newer pure play Internet companies seem to ignore this function. In this section, the auditor will determine if the QA function is present. If it is present then it will be reviewed.

2.8 Reporting. Logging of all logins, attempted intrusions, etc. must be

maintained for a reasonable period of time. In this section, the auditor will determine if these logs are maintained and for how long.

2.9 Backup. In the event of failure it is usual that the last backup be used to restore the system. In this section, the auditor will determine the frequency of backups and determine the reasonableness of this schedule.

### **3.0 Ergonomics**

At this stage the auditor becomes involved in more abstract issues. In the last section on security we could be very specific about what a system exhibiting good e-Business Health requires. In the section on Ergonomics we need to be more subjective.

To achieve this end will require the auditor to meet, not only with the system developers, but with the end-users. At times, these end-users will be current customers of the system or potential customers of the system. To this end it might be necessary to develop surveys and perform focus groups.

The goal here is nothing less than determining a "thumbs up" or "thumbs down" on the e-Business vis-a-vis other e-Businesses.

3.1 Navigability. Navigation means the determination of whether or not the site makes sense in terms of browsing it.

3.1.1 How easy is it to find something on this site? If looking for a specific product how many pages does one have to surf through to find it?

3.1.2 Is there a search engine? If so, review for correctness/completeness. Many sites do not have search engines (in this instance we are talking about a search engine to search the site only rather than the Internet). If the e-Business site exhibits depth (i.e. many pages) it becomes rather difficult

to navigate around it to find what you're looking for. If a search engine is available the auditor must check to see if what is being searched for can be correctly found.

3.1.3 Is there a sitemap? If so, review for correctness/completeness. While not required and not often found, Site Maps are one of the most useful of site navigation tools. If available, the auditor will determine correctness of this tool.

3.1.4 Are back/forward (or other) buttons provided? What tools are provided the end-user for moving backwards and forwards within the site. Is the Browser's Back/Forward buttons the only navigation tools - or did the web designers provide fully functional toolbars. If so, do these toolbars work on all pages. We have found that, of those firms audited, 10% of the pages pointed to by the toolbars cannot be found.

3.1.5 Are frames used? If so, do toolbars and other navigation tools still work.

3.2 Usability. In the end it comes down to one question really: "How usable is the web site?". In this section we ask:

3.2.1 How easy is it to use this site? While the auditor might have an opinion that might well be valid, in this section we resort to surveys and focus groups to determine the answer.

3.2.2 How useful is this site?

3.3 Content. In this section we assess the value of the information contained within the site as compared to competitive sites.

3.3.1 Is content updated regularly?

3.3.2 Is content relevant?

3.3.3 Do visitors consider content worthwhile? The auditor will use survey techniques to determine the answer to this question.

3.3.4 How does content compare with competitors? The auditor will use survey techniques to determine the answer to this question.

3.4 Search engine. While the use of search engines has declined in popularity as a way to find a site it is still an important marketing vehicle on the Web. In this section the auditor will determine where the site places when performing a search using the top ten search engines.

## **4.0 Customer Service**

The web is a doorway to the company's business. However it is just one part of the business. Tangential services must be audited as well. Customer service is one of the biggest problem areas for Net firms. There have been many well-publicized instances of shoddy customer service. It is in the company's best interests, therefore, to assess customer service within the firm vis-a-vis its web presence.

4.1 Accessibility. How easy is it for your customers to reach you?

4.1.1 Review e-mail response. How long does it take you to respond to a customer e-mail.

4.1.2 Review telephone response. How long does a customer have to wait on hold before a person answers his or her query.

4.2 e-Commerce. If your site doubles as an e-Commerce site (i.e. you sell good and/or services from your site) you need to assess the quality of this customer experience.

4.2.1 Check shopping experience. Using a "mystery shopper" approach, the auditor will endeavor to make routine purchases using the web site. Determine:

4.2.1.1 Is the shopping cart correct (i.e. are the goods you purchased in the shopping cart)?

4.2.1.2 Does the e-commerce software calculate taxes properly?

4.2.1.3 Does the e-commerce software calculate shipping charges properly?

4.2.2 Check the fulfillment experience?

4.2.2.1 Is a confirmation e-mail sent to the purchaser?

4.2.2.2 Is the return policy carefully explained?

4.2.2.3 How quickly does the company refund money on returns?

4.3 Privacy. The auditor must review the company's privacy policy statement at a minimum. He or she should then review the data flow to determine if the privacy policy is being adhered to.

## **5.0 Legality**

The digital age makes it easy to perform illegal and/or potentially litigious acts. From a corporate perspective this can be anything from a web designer illegally copying a copyrighted piece of art to employees downloading pornography.

5.1 Copyright.

5.1.1 Check the content ownership of text on your site. It is quite easy to copy text from one site to another. Ensure that your copy is completely original or that you have the correct permissions to reprint the data.

5.1.2 In the same way check image ownership.

5.2 Employee Web Usage. There have been a number of court cases where employees claimed harassment when other employees within the organization downloaded and/or e-mailed pornographic. The company is responsible for the actions of its employees therefore it is highly recommended that the company do the following:

5.2.1 Create a policy memo detailing what can and cannot be

done on the Internet (include e-mail). Make sure all employees sign and return this memo. Use tools such as those on surfcontrol.com to monitor employee Net usage.

5.2.2 Determine whether any e-mail monitoring software is used and determine its effectiveness.

## **Conclusion**

The e-Business Audit is a critical component of the e-Business plan. As you can see from this checklist the audit is extensive and quite thorough. It is recommended that it be performed at least once a year. If the e-Business site is modified continually then the Audit should be done more frequently as well.

e-Business Health depends upon many factors. Ignoring any one of them puts your e-Business at risk.

## **Author Bio:**

Jessica Keyes is the founder of New Art Technologies, Inc. New Art assists clients in improving their bottom lines through the development and implementation of strategic initiatives. Keyes is the author of 18 books and 200 articles and is a professor computer science.