Auditing in an E-commerce Environment

By: Janice Law
Friday, June 22, 2012
Table of Contents

Introduction                                                                                                                  .......................................................................................................................... 3
Defining E-Commerce                                                                                                         .......................................................................................................................... 3
Choosing the Right People                                                                                                    .......................................................................................................................... 4
Traditional Accounting Standards and Current Available Standards to Adopt                                                   .......................................................................................................................... 5
New Frameworks and Guidelines for E-commerce Auditing                                                                      .......................................................................................................................... 7
  Key Performance Indicators and Stress Testing                                                                             .......................................................................................................................... 8
  Website Auditing                                                                                                            .......................................................................................................................... 9
  Electronic Payments                                                                                                         .......................................................................................................................... 10
New Auditor and Management Focuses                                                                                              .......................................................................................................................... 11
Suggestions for Future Research                                                                                               .......................................................................................................................... 13
Conclusion                                                                                                                   .......................................................................................................................... 13
Appendices                                                                                                                   .......................................................................................................................... 15
Literature Survey                                                                                                           .......................................................................................................................... 17
Annotated Bibliography                                                                                                       .......................................................................................................................... 20
Introduction

Upon the fast evolution of technology over the past few decades, society has become quick to adapt to new products and services. Now that society is peaking at the information age, standards for the validity and reliability of information have increased as consumers are more informed and empowered than ever.\(^1\) Since people expect more high quality and timely information, it changed the way companies conduct their businesses as well. In response to this trend, electronic commerce (e-commerce) has become an increasingly popular form of business that continuously proves its success and potential, as online sales based in the U.S. are expected to reach $327 billion in 2016.\(^2\) However, businesses are not the only parties that need to incorporate e-commerce into their activities. Auditors too must consider how e-commerce will impact their line of work. More importantly, the emergence of e-commerce and its impact on changes in information technology functions increases audit risk.\(^3\) Based on the literature reviewed, there is an existing concern with regards to differences in auditing e-commerce compared to traditional commerce. To respond to this concern, this research report aims to pinpoint the changes that tradition audits are facing, and how auditors should approach these changes. To further inform auditors, existing frameworks are explored and new guidelines are recommended. Though such frameworks are specified to auditing e-commerce, they must also be combined with traditional auditing procedures to result in a successful audit. In essence, the report aims to add to current audit procedures to place sufficient focus on certain aspects that e-commerce auditing needs. Potential future management focuses and suggestions for further research are provided as well.

Defining E-Commerce

Before diving into how auditors should approach e-commerce auditing, a thorough understanding of it is crucial to identifying its need for attention. E-commerce essentially covers all types of transactions that occur in traditional businesses with the exception that it conducts these transactions online. These business activities include business-to-business (B2B), business-to-consumer (B2C), extended enterprise computing, digital commerce (d-commerce), and mobile commerce (m-commerce).\(^4\) When selling goods via e-commerce, certain software functions run the main functions of the business’s e-commerce web site which allows for product display, online ordering, inventory management, and such.\(^5\) Specifically, for the purpose of this report, understanding e-commerce from a business’ perspective is most important because auditors are auditing from the client’s perspective. Within e-business, all transactions are

---

electronic and trading partners may be temporary since exchanges are usually over a short period of time. There are three components of the business to take note of:  

1. **Technology component**: networking technologies for exchanging financial transactions; there is usually database technologies available for storing financial transaction records  
2. **Systems component**: financial and accounting systems to process financial transactions; the systems can be web-based, enterprise systems, and legacy systems  
3. **People component**: service providers (ie. audit personnel and firm personnel), and stakeholders (ie. customers, suppliers)

In conjunction with the servers and data lines, there is heavy reliance on interconnected networks in the e-commerce environment. Although e-commerce is not much different from a traditional business other than its steep integration with new technologies, all e-commerce systems have a distinct characteristic - total involvement of the end-user at every stage of the purchasing process. Despite e-commerce’s raising popularity and unique approach to conducting businesses, it continues to be vulnerable to the strain of day to day running of business transactions. As well, its lack of consumer and business confidence creates an overall fear amongst society and businesses. This being so, auditors must take action to provide more assurance towards this new area of technology by fully proving architecture models for e-commerce businesses.

**Choosing the Right People**

Since traditional audits differ from e-commerce-enabled businesses, certain audit processes have to be reconsidered when approaching audit engagements. The following are the top five factors that are necessary among auditors for successful e-commerce audits compared to traditional audits:

1. **Knowledge of organizational security vulnerabilities**  
   Vulnerabilities that are internal and external to the business, either in logical or physical nature must be identified since most businesses are highly vulnerable to security lapses and breaches.

2. **Expertise in system and network change management**  
   Auditors that were chosen to be on the engagement must have a minimum level of expertise in system and network change management. This being so, the auditors who have limited knowledge on IT systems should utilize auditors with expertise to seek vulnerabilities introduce by software in the networks.

3. **Security specialist on audit team**  
   There should be members with expertise specifically in intrusion detection, prevention, and recovery management. Although this is a complex IT expertise, it can be outsourced.

---

4. Knowledge/training in auditing of financials in integrated systems environment

During the process of planning materiality and looking into the quality of audit evidence obtained, the audit team members should have knowledge or training in auditing the financials of a highly integrated accounting environment. Because of computerized scenarios, most professional auditors should hold this expertise.

5. Experience in web site review/audit

Auditors on the engagement should possess a minimum level of experience in web site review or audits. Entities have multiple layers of web sites and portals, making WebTrust experience useful as well.

Overall, there is need for higher training levels in advanced IT methods and tools for technology auditors in rendering audit judgements. Ideally, audit teams that are responsible for an e-commerce business should meet all of the above requirements. Such characteristics of an audit team factor into the auditors’ judgement capability that indicate they are able to make decisions based on professional audit judgement while planning and managing the audit process. This is dependent on IT expertise and IT audit expertise combined, and the lack of the business process and systems training would hinder such capability. As well, audit judgement capability is crucial to the e-commerce environment as auditors need to understand how to extract the electronic transactions to ensure accurate audit assessment of those transactions. It is important for them to be involved in the design of the information systems to prevent control weaknesses from being designed into the system. If members of the team have such IT expertise and IT audit expertise, they will be able to properly conduct the audit process through knowing not only how to vouch, but what to vouch for as well.

With regards to audit risk, the e-commerce environment creates more complexities for the audit team. Based on CPAs’ perceptions, where there is material transactional e-commerce presence in the business (defined as 20% or more of sales derived from e-commerce), inherent, control, and detection risk all increase. Because of such increases in risks, further emphasis is placed on the important of an experienced and competent audit team to smooth the audit process and suppress audit risk.

**Traditional Accounting Standards and Current Available Standards to Adopt**

There are several standards and frameworks that are currently available made by associations such as the Canadian Institute of Chartered Accountants (CICA), American Institute of Certified Public Accountants (AICPA), and Information Systems and Control Association (ISACA). Frameworks have been identified by the associations to guide auditors in auditing businesses where there is heavy

---


information technology integration compared to audits done in the past. The primary and most relevant assurance tool for e-commerce is Trust Services. Issued by the CICA and AICPA, they are professional assurance and advisory services based on a core set of principles and criteria to address the risks and opportunities of IT in a business.12 Businesses that meet the standards are provided a seal, such as WebTrust and SysTrust. They are assurance seals provided to websites that have met the privacy and security standards issued by the CICA and AICPA. To aid auditors in their decision making, CICA and AICPA introduced the Trust Services Principles and Criteria that states broad statements of principles and identifies specific criteria that need to be achieved. Once the criteria are achieved, they yield the information as useful to its intended users as the criteria are benchmarks used to deem the information as objective, measurable, complete, and relevant.13 Organized into five areas, auditors in an e-commerce environment can use these criteria to decide as to whether or not the client has reliably integrated its business with its IT system and accounted for potential risks the IT system brings:14

- **Security.** The system needs to be protected from unauthorized access, both logically and physically. With e-commerce specifically, information is to be made available only to those who need the access to complete the transaction or services, or follow up on questions and issues that may arise.

- **Availability.** The system is available for operation and use as committed or agreed. This in itself does not set a minimum acceptable performance level for system availability - that is established through commitments made by mutual agreements between the related parties within the e-commerce business.

- **Processing integrity.** The system processing is complete, accurate, timely, and authorized. It should be performing its intended function in an unimpaired manner that is free from unauthorized or inadvertent manipulation.

- **Confidentiality.** Information that is being communicated and exchanged is protected as committed or agreed by the partners.

- **Privacy.** Personal information collected from the client’s customers, employees, and other individuals is used, retained, and disclosed in conformity with the commitments in the entity’s privacy notice and with criteria set forth in Generally Accepted Privacy Principles issued by the AICPA/CICA.

While the handbook establishes these guidelines in much further detail, the popular COBIT framework has also been noted to help auditors see the effectiveness of IT governance. Meeting the COBIT standards ensure that IT aligns with the business, enables the business, maximizes benefits, and uses resources responsibly.15

---


Despite the introduction of CICA’s Trust Services and ISACA’s COBIT framework for auditors to mitigate the risks of heavy IT reliance, such standards are not specific to e-commerce. Though it takes into account many aspects auditors must be careful of in an e-commerce environment, these guidelines only pertain to IT governance and integration of IT as a whole. Nonetheless these frameworks have assisted auditors throughout the emergence of technology within a business so far. However, as e-commerce is becoming more popular, more assistance and specifications need to be developed to cater to this type of business as it has catered to brick and mortar businesses in the past. Accountants have been able to overcome the learning curve in the past dealing with the integration of information technologies, and now they must do the same with the web-enabled era. Note that in 2010, e-commerce use was valued at $15.3 billion in Canada alone\textsuperscript{16}, and $173 billion in the US\textsuperscript{17}, none of which accounts for web-influenced retail sales. To this, further attention should be catered to e-commerce auditing as the industry approaches its trillion-dollar value.\textsuperscript{18}

**New Frameworks and Guidelines for E-commerce Auditing**

Before auditing a business conducting e-commerce, auditors have to consider the basic threats the business encounters the moment it begins using the internet, intranet, and any web technologies:\textsuperscript{19}

1. Unauthorized alteration of data
2. Unauthorized access to the underlying operating system
3. Eavesdropping on messages passed between server and browser
4. Impersonation

Once these four threats have been accepted in the early stages of the audit process, auditors must look into whether or not the client has security policies set in place to identify possible threats and risks. This being so, management has to have determined which assets must be protected. Not only should security policies be in place, but enforcement and educating users of the security policy is equally as important.\textsuperscript{20} Management must understand the risks in security and promote security awareness upon defining and implementing security architecture.\textsuperscript{21} If the client is unable to present security policies, initial audit risk may be too high for client acceptance.

\begin{itemize}
\end{itemize}
Key Performance Indicators and Stress Testing

Once the auditor and client decide to proceed with an audit, the next step in the audit process involves collecting and analyzing audit evidence. The basis of evidence collection is different in the case of an e-commerce business. Because e-commerce businesses derive all of its sales through its website, analysis is focussed primarily on transactions and interactions between its application server and client computers, as opposed to tracking employee procedures and physical controls where traditional businesses use a brick and mortar platform to reach customers. Auditors can use key performance indicators to track the behaviour of the web server and use the indicators to identify how stable the server is since the web-server is arguably the most crucial component of an e-commerce business. Such indicators include:22

- Workload limit with stable performance
- Hourly performance of a system
- Daily performance of a system
- Problems in process definition
- Identification of cancelled process instances or activity instances

Upon identifying the indicators in relation to the client’s web activities, likelihood of system failure can be seen by the auditor. Normally, audit trail data is analyzed to see the efficiency of the web-server. However, that only provides an internal perspective of how well the web-server works. By using these key performance indicators, business process engineers can view the business from an internal and external point of view to control bottlenecks in traffic to overcome the risk of server crashes due to flash crowds.23

In the case that auditors choose to become a part of the design process, use of the indicators would help create a higher quality web system. Knowing this information allows the auditor to assess the amount of IT risk involved based on how well the business can handle traffic, and how efficiently it can reboot its functions in the case of system failure. Another tool that is useful in assessing stability of the web-server is stress testing. Stress testing presents an external view of the web-server and recognizes the capability of a web-server in handling massive simultaneous requests using simulation of intensive traffic.24 Using these tools that focus on the likelihood of failure in the web-server in e-commerce would be highly beneficial. In addition, many web-enabled businesses nowadays integrate Web 2.0 into its e-commerce to allow consumers to generate product awareness or further marketing efforts. Since Web 2.0 creates more risks on the external side of the business, it is important to incorporate safeguards that consider both management’s control frameworks and the IT developer’s control techniques.25 (See Appendix 1)

Often times, audits overlook the client’s web interface and functionality although emphasis on this aspect of a business is important when auditing in an e-commerce environment.

---

Website Auditing

Aside from the concerns of the design and maintenance of the client’s web server, issues also arise from the mere existence and use of a website as well. Website audits are another strategy to ensuring e-commerce functionality, as it is the client’s website is the most critical component of the business. Unlike traditional businesses, e-commerce products and services are available on a 24-hour basis. Because of its lack of downtime, there are more gateways to miscreants. Security and application integrity cannot be emphasized enough as 25% of small to medium-sized businesses have been subject to a security breach in their IT system in 2010.26 Also, there are much shorter application developments in an e-commerce environment because of the natural urgency to have to enter the market as soon as possible. Therefore, management has to be careful to not skip steps in the development process to ensure a website that has endurance. Lastly, conducting business online allows for more international activities due to the lack of costs to do so. Because websites have a wide reach, it naturally exposes the company not only to customers, but also competitors and organizational critics. This calls for the need for increased content review due to the likelihood of scrutiny for legal and publishing purposes. The company has to not only ensure it is not breaching legal policies, but that its content is not offensive or culturally insensitive as well.27

As the audit team gathers knowledge upon the client’s business operations and where points of failure can occur, process mining is a useful procedure to take. The goal of process mining is to extract information from event logs recorded by an information system. Information from event logs has data stored from information systems.28 Given the event logs, process mining tools create a process model consistent with the observed dynamic behaviour of the business. Use of the model extracted from process mining allows auditors to find deviations of the actual events occurred with the predefined models. An illustration in Appendix 2 can provide a greater understanding as to how process mining can display how the client’s information system represents the business’s actual events. Any deviations that have been identified will allow the auditor to evaluate the adequacy of the client’s information system for the purposes of its e-commerce activities. The quality of the client’s information system is crucial as e-commerce involves heavy electronic data processing. More importantly, it shows the auditor the degree of reliability and accuracy of audit evidence that is being pulled from the client’s information system.

Electronic Payments

Incoming information from the customer’s side of the business would be overlooked if an e-commerce business was to be audited with traditional procedures. Specifically, electronic payments are inherently a large part of the business to audit due to the nature of e-commerce. Traditional audits view incoming money in a much simpler way than they should be since various types of payments have been made available. In the chain of data access for cash transferral, other parties aside from the client include consumers, payment processors, banks, and credit card issuers.²⁹ Because of the many involving parties and several potential points of failure, it is important to consider which party takes the ultimate responsibility of any loss in breaches of security. If the client decides to rely on an outside party to take on any responsibilities, auditors should ensure the client has adequate, detailed agreements in place with the third parties to relieve the client of its financial burden and risk. In addition, adequate design of the client’s electronic payment systems must be reviewed since it is likely to be the transferral method of cash the company receives. The following is a list that includes several factors to consider in an electronic payment system design³⁰:

1. Privacy: Users expect trust in a secure system.
2. Security: A secure system that verifies the identity of two-party transactions through user authentication. It has to have flexibility to restrict yet provide information/services through access control
3. Intuitive interfaces: The payment interface has to be simple enough for customers to navigate on their own without prior experience
4. Database integration: Integration with various databases such as financial institutions, third-party payment systems, and credit card issuers
5. Brokers: A “network banker”, someone to broker goods and services, settle conflicts, and financial transactions electronically, must be in place.
6. Pricing: How to price payment system services. For example, from cash to bank payments, or from paper-based to e-cash. Services charges have to be set in place.
7. Standards: Without standards, the welding of different payment users into different networks and different systems is impossible.

Reviewing the design of the system decreases detection and control risks in future audits. As well, having an adequate electronic payment system provides assurance that the client will not encounter any problems in the money transferral process to hinder collection of revenues. Emphasis is placed on this for the reason that e-commerce relies on this system only to receive its money.

New Auditor and Management Focuses

Breslawski’s study suggests that CPAs perceive audit risks and costs to increase moderately where there is material e-commerce presence within a company. Where e-commerce accounts for more than 20% of sales and 20% of purchases, the raise in inherent, control, and detection risks suggest changes in the audit practice is necessary. Before diving into methods to mitigate the increase in audit risk, perceived risk in an audit may change the need to mitigate at all. Theoretically, the idea of risk only goes as far as it can be perceived, meaning auditors can only measure the level of risk based on the amount of assurance they are given. This being so, if there is perception that data assurance has increased, audit risk is perceived lower as well. Thus, in electronic exchanges, high supply of data assurance is crucial for the auditor to judge the client’s performance and level of risk. Providing data assurance directs back to the idea of using any of the frameworks and guidelines mentioned above. And so, to begin mitigating the increase in audit risk, the auditor must ensure enough data assurance is present.

Management can choose to perform continuous monitoring on its e-commerce business. This is not to be confused with continuous auditing since the process falls under management’s responsibility. Essentially, the key business process transactions and controls are constantly assessed. However, in conjunction with continuous audit, performing the bulk of regular testing activities can free up the audit team to focus on the more critical processes that affect the company as a whole. Although continuous monitoring was imposed by Sarbanes-Oxley in the past, it is expected to be one of the areas to have the greatest impact on audit going forward. To appropriately implement continuous auditing and monitoring to reap the greatest benefits, management must overcome the lack of appropriate software, gathering expertise, and responding to exceptions. The most important aspect of implementing continuous monitoring is providing leadership and assigning responsibility roles to members of the business to ensure the approach is fully integrated with the overall audit strategy. In addition, audit and management can established a new working relationship through reaching further understanding of the company. This approach mitigates the increases in audit costs as well. One audit organization reported a combined savings of $21 million in one year through using audit analytics and continuous monitoring, as another reported annual savings of nearly $1 million based on a decrease in incorrect billings alone.

Returning to the idea that electronic payments are a substantial part of an e-commerce client, the use of credit cards has become an increasingly notable form of payment as well. Due to the increased convenience and financial benefits credit card issuers are providing, credit card payments experienced a 10.7% annual growth in 2011.38 This statistic is to be highlighted for clients that perform e-commerce since customers either pay through credit cards or electronic transfers. Clients themselves normally purchase its needs on account as well. While the risks of electronic transfers can be mitigated by contractual agreements as mentioned above, management must have controls and processes in place to avoid audit failure in the payment card industry. Customers expect confidentiality and credit card institutions demand compliance. The following is a list of guidelines management should follow to ensure all parties’ needs are met:39

1. Justify the storage of credit card data. Determine where credit card data is stored in the organization, what the data is used for, and whether it is needed there. It is also essential that legacy reports have been modified to remove data that is no longer needed.

2. Third-party conduct application test and code review: This ensures that the custom Web applications are securely coded.

3. Document the flow of credit card data through the organization.

4. Incorporate encryption at the development phase.

5. Use a company-wide encryption strategy.

6. Continually educate and train internal staff.

The strategies listed above are only few of several techniques management can follow to escape common audit failures in relation to incorporating credit cards as a method of receivables. Refer to Appendix 3 for the full list of available strategies.

Although e-commerce is seemingly a genius technology for businesses to exploit consumerism, the industry continues to be suppressed by technological restraints. E-commerce is vulnerable to the strain of business transactions run on a daily basis where massive volumes of data are involved. Regular audits can provide assurance, but the basis of a successful e-commerce business incorporates control mechanisms on management’s behalf. Based on interviews conducted to help build a framework for managing e-commerce security, specific controls have been identified for management to implement:40

1. Strategic controls: E-commerce steering and project committees should participate in audits.

---


2. Development controls: This includes proper selection of secure and reliable e-commerce platform and infrastructure. Any changes in the e-commerce system should be highly regulated and proven effective.

3. Operational controls: Regular security reviews, e-commerce disaster recovery planning, and access control policies for customers should be available and enforced by management.

In addition, acceptance of external information should be controlled. The following framework provides guidelines for controls that pertain to e-commerce occurrences specifically:\(^{41}\)

1. Operational controls: This includes customer validation, acknowledgment of transactions, e-commerce audit trails and logs, and demilitarized zones.

2. Internet controls: Secure payment gateways, firewalls, and encryption should be in place.

3. Customer controls: Digital certifications/signatures, and two-phase authentications should be required upon verifying customer legitimacy and acceptance.

Suggestions for Future Research

Numerous frameworks and guidelines have been reviewed and implemented over the past decade to tackle complications e-commerce brings in the auditing practice. This new technology calls for further research to verify the true effectiveness of the guidelines that have been provided. Conducting research studies to test the impact, both financially and operationally, of implementing these guidelines would make them more convincing to current e-commerce businesses and those that wish to pursue e-commerce in the future. It would also be helpful to quantify the differences in costs for e-commerce centered audit procedures compared to traditional audit procedures. Even more, a cost benefit analysis of trading in one audit technique for the other would be helpful in exploring whether audits should even be conducted differently for e-commerce in the first place.

Conclusion

This research report has brought upon several new frameworks and guidelines that can be used most effectively in conjunction with existing guidance used currently. One of the key takeaways for auditors engaged with clients in an e-commerce environment is to ensure the client’s web interface and electronic payments are not overlooked. Auditing the web server and its integration with the business is essential where physical inspection, arguably the most reliable audit evidence, is nearly impossible. At the same time, design and development of the e-commerce system as a whole must be considered as it likely has the highest impact on the future longevity of the client’s business. For a business that is so heavily based on this new technology, any collapse in the technological aspect will lead to potential business and audit failure. Though there are many mechanisms available, auditors will continue to face many risks and

---

challenges to provide audit opinions that are most representative of the clients in the new area of business.
### Appendices

#### Appendix 1

<table>
<thead>
<tr>
<th>Safeguards</th>
<th>Affected Area</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Implement a robust policy governing the use of Web 2.0 applications.</td>
<td>Policy implementation</td>
</tr>
<tr>
<td>2. Educate users on the risks associated with Web 2.0 applications and</td>
<td>User-education</td>
</tr>
<tr>
<td>related safeguards.</td>
<td></td>
</tr>
<tr>
<td>3. Monitor and review resource activity, as well as following up on all</td>
<td>Monitor and review</td>
</tr>
<tr>
<td>logs and audit trails.</td>
<td></td>
</tr>
<tr>
<td>4. Ensure that all network and software (including the latest patches)</td>
<td>Network security</td>
</tr>
<tr>
<td>are frequently updated.</td>
<td></td>
</tr>
<tr>
<td>5. Utilise all browser security features and ensure the browser is</td>
<td>Browser security</td>
</tr>
<tr>
<td>correctly configured.</td>
<td></td>
</tr>
<tr>
<td>6. Utilise all security features that the Web 2.0 application has available</td>
<td>Program security</td>
</tr>
<tr>
<td>and ensure that the application is correctly configured.</td>
<td></td>
</tr>
<tr>
<td>7. Implement input validation and other technological driven controls.</td>
<td></td>
</tr>
<tr>
<td>8. Sign a service level agreement with service providers of frequently</td>
<td></td>
</tr>
<tr>
<td>used Web 2.0 applications.</td>
<td></td>
</tr>
<tr>
<td>9. Block access to designated websites, file types and utilities.</td>
<td>Security software</td>
</tr>
<tr>
<td>10. Implement a next generation reputation based filtering of all forms of</td>
<td></td>
</tr>
<tr>
<td>incoming and outgoing communications.</td>
<td></td>
</tr>
<tr>
<td>11. Utilise deep-scanning heuristic and behavioural antimalware programs.</td>
<td></td>
</tr>
<tr>
<td>12. Review the source code of frequently used websites and remain</td>
<td>Development and maintenance</td>
</tr>
<tr>
<td>involved in the open-source community and search support websites for</td>
<td>controls</td>
</tr>
<tr>
<td>vulnerabilities.</td>
<td></td>
</tr>
<tr>
<td>13. Develop a best practices framework for the utilisation and creation</td>
<td></td>
</tr>
<tr>
<td>of Web 2.0 applications.</td>
<td></td>
</tr>
</tbody>
</table>


#### Appendix 2

![Diagram](Diagram.png)

## Appendix 3

<table>
<thead>
<tr>
<th>Action</th>
<th>Description and Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Justify the storage of credit card data</td>
<td>Determine where credit card data is stored in the organization, what it is used for, and whether it is needed there. In addition, be sure that legacy reports have been modified to remove data that is no longer needed.</td>
</tr>
<tr>
<td>Document the flow of credit card data throughout the organization</td>
<td>Understand where data goes—from the point where you acquire it (either from a customer or third party) to the point where the data is disposed or leaves the network.</td>
</tr>
<tr>
<td>Incorporate encryption at the development phase</td>
<td>Use an encryption framework during development instead of developing applications and then retro-fitting them for encryption.</td>
</tr>
<tr>
<td>Have a company-wide encryption strategy</td>
<td>A typical company has multiple encryption requirements—for everything from virtual private network (VPN) tunnels using Secure Internet Protocol (IPsec), email secured by Secure/Multipurpose Internet Mail Extensions (S/MIME), and Secure Sockets Layer Certificates (SSL Certificates), to mainframe, database, and disk encryption (e.g., for users with laptops).</td>
</tr>
<tr>
<td>Update software with patches as they are released</td>
<td>Ask the POS application vendors whether their current- or older-version applications store track data. Validate their statements by testing the application or looking for third-party validation of the output and data stores.</td>
</tr>
<tr>
<td>Have a third party conduct an application test and code review to ensure that custom Web applications are securely coded</td>
<td>Improve internal software development life-cycle practices by integrating security into these cycles.</td>
</tr>
<tr>
<td>Perform quarterly scans as required by the PCI standard.</td>
<td>Delegate a representative to be part of the SDLC process. Then document the relevant processes to verify that the application development team performed risk analysis, set security requirements, performed requirements testing, and so forth.</td>
</tr>
<tr>
<td>Avoid ad hoc development, implement replicable processes, and document everything</td>
<td>Develop processes that ensure adherence to security procedures and policies.</td>
</tr>
<tr>
<td>Continually educate and train internal staff.</td>
<td>Doing so helps ensure that they will detect the types of activity you are most concerned with.</td>
</tr>
<tr>
<td>Place IPS/IDS near the assets you want to protect</td>
<td>Doing so helps ensure that the devices will detect types of activity you are most concerned with.</td>
</tr>
<tr>
<td>Establish a centralized server for reviewing, correlating, and managing IPS/IDS logs.</td>
<td>Log management technology, security information management technology, and managed log services provide some or all of the required functionality. Centralized solutions also enable monitoring who has access to credit card data and, in ideal cases, track the workflow of log review activities.</td>
</tr>
<tr>
<td>Place dedicated wireless IPS devices near the assets to protect</td>
<td>Some of the log collection, normalization, and correlation can be outsourced, but at some point, someone from the company must review the reports to determine whether there are any risks to credit card data.</td>
</tr>
<tr>
<td>Configure PCI–relevant systems to log the data elements specified in requirement 10.2, and use a system to centralize log collection, aggregation, and reporting</td>
<td>Make sure that you can get to the logs easily and that they are tracking necessary access data. In addition, be sure that they do not store credit card data in clear text.</td>
</tr>
</tbody>
</table>


**Literature Survey**

The basis of this research paper stems from the recognition of rapid changes in the auditing field as e-commerce enabled businesses involve different business processes compared to traditional businesses. The key aim of the survey was to explore research and studies previously performed that pertains to the topic at hand. Specifically, issues that surround e-commerce and changes in audit had to be identified and verified for this research paper to be valid. The new business environment that recent technology provides is encouraging auditors to explore various auditing methods to achieve minimum audit risk. These papers prove that new risks and mitigation of such risks in fact exist in the current environment.

Upon reading various research papers and scholarly journal articles, there are multiple perspectives on the association between the field of auditing and using the internet as a means to conduct business. Since the integration of information technology in an e-commerce environment is heavy, studies show that information technology highly impacts the internal auditing process. Increase in risk could occur if appropriate applications and guidelines are not applied. (Moorthy, Mohamed, Gopalan, and San 2011) Although auditing standards specifically tailored for technology auditing have not been made, creating effective auditing tools can help increase the efficiency and productivity of IT systems. Companies that rely heavily on IT to conduct its e-commerce can greatly benefit from proper auditing of their IT systems.

Several studies place emphasis on surveys and opinions based on certified accountants in order to gain perspective on how e-commerce truly affects auditing in real-world scenarios, as opposed to theoretical studies. For one, a survey was also conducted to identify critical success factors amongst CPA’s and CA’s with regards to e-commerce auditing. (Pathak, Hussein, and Ahmad 2008). As well, information on audit risk was vouched for in a more in-depth study that reviewed the aspect of audit risk. Concluded that e-commerce transactions increase overall audit risk from studies derived from CPA as subjects (Breslawski 2007), it is important to explore frameworks and guidelines that will assist auditors in mitigating such increases in audit risk. As Breslawski attempts to provide such frameworks and guidelines, the causes for such increase in audit risk have been identified. Such causes are recognized by Jin Hong, in his discussion of risk management for auditors in e-commerce. Specifically, additional risks to the business are triggered as businesses tap into the blue ocean of e-commerce. Auditors now have to tackle technology risks and moral hazard risks that are naturally associated with e-commerce-enabled businesses. (Hong 2011) To this, numerous risk management methodologies have been explored to mitigate such risks from internal management’s perspective. (Hong 2011) With information as to how management can approach these risks, auditors can incorporate this knowledge into their procedures as well.
Since e-commerce poses a different approach associated with what businesses consider to be cost-effective and efficient, key performance indicators have been identified to help auditors judge what the business can and cannot withstand. Because web-enabled businesses often experience high-traffic situations, such indicators can provide much insight for the auditors. (Pun, Si, and Pau 2012)

While the research paper aims to pose guidelines as to how auditors can evaluate the company’s activities, consideration must also be taken to what occurs to the business from a going-concern basis. In using the key performance indicators provided, recommendations to the business can be highly valuable. In addition, the key performance indicators can help both internal management and auditors to keep the process failure risk as low as possible, through building a system that best suits the behaviour of the incoming traffic. The auditor can use these for the future planning of the web system the business has in place. Continuous improvement of the website development strategies and server maintenance routines is essential to businesses that perform e-commerce.

Another important aspect of e-commerce is its users. Since data exchange is constantly occurring in e-commerce, the users’ perception of risks in the exchange impacts how well the system is maintained. Note that users are only able to perceive the system’s performance, and not actually assess it. In order to gain users’ acceptance and trust when evaluating the system, there must be transparency for the user and proper data assurance communicated. (Nicolaou 2010) Essentially, data assurance helps absorb users’ uncertainty towards the system. Doing so will increase perceived performance outcome of the system, thus making the system seem more reliable. This study helps auditors ensure to users of the audit report that data exchange within the company is in good state. Often times the most reliable source of assurance is perception. This means people cannot fully assess how “great” a system is- they can only make assumptions on its potential to failure (until they actually experience it). In order to make educational assumptions, people use assurance as a means to justify that a system is unlikely to fail. The higher the assurance provided, the more likely a person is to believe the system truly works. This belief is what auditor can leverage on to convince users of the audit report that the likelihood of failure is low. Since user’s perception of risk impacts the auditor’s perception of risk, it is important to capture users’ perceptions.

It would be useful to further expand this study by incorporating the actual causes of data exchange failure rate to the existence of assurance seals for the system. Since results suggest that perception of risk is negatively correlated to perception of performance outcome, there should be closure as to whether it is negatively correlated to actual performance outcome as well. Although this should be the case, it is possible that perceived risk is not related to performance outcome at all. If so, though unlikely, assurance seals would lose its effectiveness and credibility.
An interesting approach to assessing the quality of an e-commerce system was conducted through the use of ISO 9126 framework and belief networks. In a research paper conducted by Stefanis and Xenos (2011), a new model was formulated for assessment based on external and internal characteristics e-commerce quality consists of. This highly technical approach surveyed users and asked the subjects to consider how much a specific characteristic catered to the idea of “quality in e-commerce”. Then, assigning each characteristic to a node, the Bayesian Networks was used to pinpoint which characteristics attributed to true quality. Research papers like these allow auditors to develop generic models to determine the actual value of a business system. Aside from an e-commerce auditing perspective, such models can help assess various aspects of a system. By placing different characteristics of an area for assessment in the nodes, people can begin to seek the true value of a system. This is similar to using the value of the sum of its parts to determine the overall value. New models like this allow auditors and management to properly assess their systems and how well it serves the business’s purpose, either from a going-concern or competitive advantage basis. Even though auditors may not be concerned with how long the system will last strategically speaking, knowing the quality of it is very helpful for their cause.

The research papers mentioned above were a portion of the papers that have been reviewed for the purposes of this research report. The papers provided different perspectives on the topic of auditing for e-commerce. It generated new and identified existing frameworks and guides for auditing from both the internal and external perspective, and considered the several types of related risks. Studies provided insight on the multiple stages within e-commerce, such as planning, development, performance, and review. The knowledge of these stages can provide efficiency in the audit engagement by helping auditors understand more about this new emerging form of business. More importantly, auditors can become more concise regarding the audit opinion they are to issue.

Upon the numerous topics surrounding e-commerce, the general idea drawn regarding the need for e-commerce auditing techniques is consensual. That is, higher audit risk is associated with e-commerce auditing, and auditors need to begin adapting new frameworks for this.
### Annotated Bibliography

<table>
<thead>
<tr>
<th>Author</th>
<th>Title of Article</th>
<th>Periodical/Website</th>
<th>Vol./No./Edition</th>
<th>Year Published</th>
<th>Date Accessed</th>
<th>Location, Database, Website Link</th>
<th>Added to Final Paper?</th>
</tr>
</thead>
<tbody>
<tr>
<td>A. Stefani and M. Xenos</td>
<td>E-commerce System Quality Assessment Using a Model Based on ISO 9126 and Belief Networks</td>
<td>Software Quality Journal</td>
<td>Vol. 16, Issue 1, Pg. 107-129</td>
<td>March 2008</td>
<td>May 10(^{th}), 2012</td>
<td>Computer and Information Systems Abstracts</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Annotation**

The paper proposes that enhancing the level of transparency within a web-based system would enhance assurance signals communicated to its users. Essentially, data assurance relates to the level of transparency perceived within transaction and processing controls. Results show that third-party certification services can be substituted by supply of data assurance. The research study assigns its subjects to measure its expected transaction performance after judging their perceived risk going into the web-based exchange. In measuring their perceptions of data assurance, results are as follows:

1. Situational risk significantly influences risk perceptions in a data exchange
2. Presence of transparency assists user control decision uncertainty and reduces perceived risk
3. Perceived risk has a negative influence on the attainment of expected performance outcomes
4. The degree of situational risk has significant effect on perceived risk, but is moderated by presence of data assurance

Data assurance is motivated by the need to provide control signals in a web-based data exchange, thus, justifying the demand for assurance as a means to absorb uncertainty.

In recognizing that E-systems are transitioning into the new economy of business, a new model has been proposed to help evaluate the quality of these
applications. Essentially, the paper attempts to break down E-commerce into its primary characteristics and using Bayesian Networks and ISO 9126. ISO 9126 is a quality standard for software product evaluation and provides quality characteristics and guidelines for their use:

![Diagram of ISO 9126 and quality characteristics]

Through assessments made by the end-users of the e-system, use of Bayesian Networks makes it possible to define the relation between various variables and estimate the consistency of the quality of an e-commerce system. It allows for forward prediction as well as backward assessment. Backwards use of model created helps the developer of the system identify the causes of the effect, while forward use of the model provides probability values for the external quality measures.

<table>
<thead>
<tr>
<th>Author</th>
<th>Title of Article</th>
<th>Periodical/Website</th>
<th>Vol./No./Edition</th>
<th>Year Published</th>
<th>Date Accessed</th>
<th>Location, Database, Website Link</th>
<th>Added to Final Paper?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Author</td>
<td>Title of Article</td>
<td>Periodical/Website Vol./No./Edition</td>
<td>Year Published</td>
<td>Date Accessed</td>
<td>Location, Database, Website Link</td>
<td>Added to Final Paper?</td>
<td></td>
</tr>
<tr>
<td>--------</td>
<td>------------------</td>
<td>-----------------------------------</td>
<td>----------------</td>
<td>---------------</td>
<td>----------------------------------</td>
<td>---------------------</td>
<td></td>
</tr>
<tr>
<td>Ch. Deepthi</td>
<td>E-Commerce</td>
<td>Sree Chaitanya College of Engineering</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Website Edition Published Accessed Website Link Paper?</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ch. Deepthi</td>
<td>E-Commerce</td>
<td>Sree Chaitanya College of Engineering</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Website Edition Published Accessed Website Link Paper?</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>D. Prashland, and A. Run</td>
<td>Processing Mining: A New Technique For EDP-Auditing?</td>
<td>Erasmus University Rotterdam</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Enright, Allison</td>
<td>Global E-commerce To Reach $1.4 Trillion in 2015</td>
<td>Internet Retailer</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Annotation
Using a variety of institution-based trust mechanisms, trust and dependability perception of electronic transactions are examined. In order to contribute recommendations for web design and optimisation of online services, the following factors used in the study:

1. Security of transaction
2. Reputation of the company
3. Web quality
4. Perception of confidentiality

In the study, it is concluded that the mere presence of seals in itself is not important for the beliefs of trustworthiness and dependability of a website. Security seals have a significant effect on users’ perceptions when accompanied by other seals. Information on a company’s legal compliance, appearance of the website’s security arrangements, and online comments all contribute to strong trust.

<table>
<thead>
<tr>
<th>Author</th>
<th>Title of Article</th>
<th>Periodical/Website</th>
<th>Vol./No./Edition</th>
<th>Year Published</th>
<th>Date Accessed</th>
<th>Location, Database, Website Link</th>
<th>Added to Final Paper?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Indvik, Lauren</td>
<td>U.S. Online Retail Sales to Reach $327 Billion by 2016</td>
<td>Mashable Business</td>
<td></td>
<td>February 2012</td>
<td></td>
<td><a href="http://mashable.com/2012/02/27/ecommerce-327-billion-2016-study/">http://mashable.com/2012/02/27/ecommerce-327-billion-2016-study/</a></td>
<td>Yes</td>
</tr>
<tr>
<td>J. Hong</td>
<td>Risk Management and Audit for E-Commerce</td>
<td>International Conference on Future Computer Science and Education</td>
<td>Pg. 601-603</td>
<td>August 2011</td>
<td>May 9th, 2012</td>
<td>IEEE Xplore: Digital Library</td>
<td>No</td>
</tr>
</tbody>
</table>

Annotation
The use of e-commerce is heavily involved with technology risk as well as moral hazard. Technology risks can be divided in four parts:

1. Risk from hackers
2. Risk from peeps
3. Risk from structural defects
4. Risk of drawbacks from information systems for companies

As for moral hazard, information asymmetry is the core cause and also divided into four parts:
1. Repudiation
2. Fake web pages
3. Privacy violation
4. Accuracy of information

Bringing in new risks for enterprises and customers, companies must incorporate new risk management. Amongst the important objectives of auditing, validity and reliability of information has become a vital part of accounting when it comes to the external auditing perspective of E-commerce. To address the special characteristics of risk in E-commerce (lack of historical information risk and dynamic risk preventions due to consistent improvements in IT), three types of risk management include:
1. Identification and evaluation of security for information systems of companies
2. Culture management
3. Disaster recovery plan

---

**Annotation**

The study surveyed auditor respondents with minimum two to three years of experience to obtain information as to what the critical successful factors (CSF) are when performing e-commerce audits. Amongst these CPA’s and CA’s, the top ten critical success factors are as follows:

1. Knowledge of organizational security vulnerabilities
2. Expertise in system and network change management
3. Security specialist on audit team
4. Knowledge/training in auditing of financials in integrated systems environment
5. Experience in web site review/audit
6. Training in the technical aspects of web site review and audit
7. Knowledge of B2B partner agreements
8. Basic training in various OS programming tasks
9. Establishment of audit objectives by audit team
10. Minimum experience of auditing/reviewing the outsourced software
<table>
<thead>
<tr>
<th>Author</th>
<th>Title of Article</th>
<th>Periodical/Website</th>
<th>Vol./No./Edition</th>
<th>Year Published</th>
<th>Date Accessed</th>
<th>Location, Database, Website Link</th>
<th>Added to Final Paper?</th>
</tr>
</thead>
</table>

**Annotation**

Many web-enabled applications are executed in workflow management systems: systems that “completely define, manage, and execute workflows through the execution of software whose order of execution is driven by a computer representation of workflow logic”. Statistics indicating success or failure of these executions are not available in audit trail data and web server logs during high-traffic situations. Though techniques like stress testing can be used to provide an external view of the application, it does not provide business insight within these applications, as audit trail analyses would. The study calculates key performance indicators through audit trail analyses, web server logs, and stress testing statistics. The key performance indicators are as follows:

1. Workload limit with stable performance
2. Hourly performance of a system
3. Daily performance of a system
4. Problems in process definition
5. Identification of cancelled process instances or activity instances

Using these indicators will allow both external/client and internal/server view of evaluating web-enabled business processes. It will assist in business process reengineering, load balancing, and implementation of contingency measures when traffic-intensive situations occur.

<table>
<thead>
<tr>
<th>Author</th>
<th>Title of Article</th>
<th>Periodical/Website</th>
<th>Vol./No./Edition</th>
<th>Year Published</th>
<th>Date Accessed</th>
<th>Location, Database, Website Link</th>
<th>Added to Final Paper?</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Author</th>
<th>Title of Article</th>
<th>Periodical/Website</th>
<th>Vol./No./Edition</th>
<th>Year Published</th>
<th>Date Accessed</th>
<th>Location, Database, Website Link</th>
<th>Added to Final Paper?</th>
</tr>
</thead>
</table>

The requirements of e-commerce in a business:

1. Electronic infrastructure
2. Legislation and regulations for e-commerce
3. Availability of human resources

The characteristics of e-commerce:

1. The disappearance of paper documents in commercial transactions
2. Inability to identify contractors
3. Products delivered electronically
4. Absence of direct relationship between the contracting parties
5. The presence of the electronic mediator
6. Speed in the completion of business transactions
7. Collective interaction between several parties

The main findings of the study show that presence of e-commerce in a business requires the use of a greater number of auditors as well as increased complexity of processes in the audit. There needs to be wider effort in audit processes and greater amount of evidence obtained in order to confirm e-commerce operations.

<table>
<thead>
<tr>
<th>Author</th>
<th>Title of Article</th>
<th>Periodical/Website</th>
<th>Vol./No./Edition</th>
<th>Year Published</th>
<th>Date Accessed</th>
<th>Location, Database, Website Link</th>
<th>Added to Final Paper?</th>
</tr>
</thead>
</table>

**Annotation**

The article attempts to address several issues of information technology and internal auditing. While IT adoption is creating more controlled environments in the auditing processing, there are still many questions for an organization to answer as it evaluated risks involved with using IT in the audit. There are four applications necessary to ensure the use of IT is successful in internal audits:

1. Software and hardware to assist the auditing process
2. Guidelines available to best practices
3. Accounting standards – audit task and mitigate organizational risk
4. Role of internal auditor – necessary skills and competence

Noting that there is no generic model for technology tools used in organizations, effective use of audit technology tools is helping change the shape of auditing approaches. In identifying the role, impact, and risk of IT towards auditors, IT will allow for increase in efficiency and productivity.

<table>
<thead>
<tr>
<th>Author</th>
<th>Title of Article</th>
<th>Periodical/Website</th>
<th>Vol./No./Edition</th>
<th>Year Published</th>
<th>Date Accessed</th>
<th>Location, Database, Website Link</th>
<th>Added to Final Paper?</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Author</th>
<th>Title of Article</th>
<th>Periodical/Website</th>
<th>Vol./No./Edition</th>
<th>Year Published</th>
<th>Date Accessed</th>
<th>Location, Database, Website Link</th>
<th>Added to Final Paper?</th>
</tr>
</thead>
</table>
Pathak, Jagdish  
An E-Business Audit Service Model in the B2B Concept  
Information Systems Management  
Vol. 27, No. 1, Pg. 59-72  
February 2010  
April 5th, 2012  
Yes

Annotation
Web 2.0 is a system of web-based communities and host servers that allow sharing and collaboration between its users. It allows users to create, collaborate, and share information on a real-time basis, consisting of three components:

1. Community and social: dynamic software that allows users to study, change, and improve content
2. Technology and architecture: runs on a web browser and does not require installation, specific device, or platform
3. Business and process: software delivered as a service rather than an installed product

Upon obtaining an understanding of technologies that drive Web 2.0 applications, the study develops a framework to identify the security issues an organization exposes itself through Web 2.0 applications. The issue is that control techniques are implemented by IT professionals, whereas management implements a control framework and models and both parties do not understand the other party's output. This is known as the IT Gap. Essentially, risk management is not merged with technical policies and procedures. In creating a comprehensive security program that merges the two, it must include the following:

1. Multi-layer approach relying on technological safeguards and security protocols
2. A Web 2.0 policy should be formulated; implemented and compliance with the policy should be monitored
3. Users need to be trained on acceptable practices and features

Author  
Title of Article  
Periodical/Website  
Vol./No./Edition  
Year Published  
Date Accessed  
Location, Database, Website Link  
Added to Final Paper?

R. Rudman  
Using Control Frameworks to Map Risks in Web 2.0 Applications  
Accounting and Management Information Systems  
Vol. 10, Issue 4, Pg. 495-515  
December 2011  
May 13th, 2012  
ABI/Inform Global

Annotation
Web 2.0 is a system of web-based communities and host servers that allow sharing and collaboration between its users. It allows users to create, collaborate, and share information on a real-time basis, consisting of three components:

1. Community and social: dynamic software that allows users to study, change, and improve content
2. Technology and architecture: runs on a web browser and does not require installation, specific device, or platform
3. Business and process: software delivered as a service rather than an installed product

Upon obtaining an understanding of technologies that drive Web 2.0 applications, the study develops a framework to identify the security issues an organization exposes itself through Web 2.0 applications. The issue is that control techniques are implemented by IT professionals, whereas management implements a control framework and models and both parties do not understand the other party's output. This is known as the IT Gap. Essentially, risk management is not merged with technical policies and procedures. In creating a comprehensive security program that merges the two, it must include the following:

1. Multi-layer approach relying on technological safeguards and security protocols
2. A Web 2.0 policy should be formulated; implemented and compliance with the policy should be monitored
3. Users need to be trained on acceptable practices and features

Author  
Title of Article  
Periodical/Website  
Vol./No./Edition  
Year Published  
Date Accessed  
Location, Database, Website Link  
Added to Final Paper?

R. Venkatesh and J. Armitage  
Accountants’ Awareness and Perceptions About Assurance On XBRL Financial Statements  
Journal of Applied Business Research  
Vol. 28, No. 2, Pg. 145-154  
April 2012  
May 8th, 2012  
ProQuest  
Yes

Annotation
Extensible business reporting language (XBRL) is used to create financial and business reports for cost savings purposes and integration of corporate governance and transparency. Even though errors and misrepresentation of company disclosures can occur with the use of XBRL, SEC does not require third party assurance on XBRL documents. As the use and impact of XBRL is increasing on audit and assurance, accountants’ opinions on the use XBRL was investigated to seek the actual importance and level of knowledge of the language. Accountants who participated in the study strongly believed that auditing methods should be adjusted to incorporate the use of XBRL information in the audit process. In addition, participants concluded that accuracy and completeness are the most important assertions, while validity and well-informedness are the least. However, the study reveals that auditors themselves have limited knowledge on XBRL, thus changing the actual influence XBRL could have on the audit profession.
Annotation
The research paper aims to answer the following questions:
1. From an auditor’s point of view, what is a material e-commerce presence?
   a. Sales exceeding 20%
   b. Purchases exceeding 20%
2. How does a material e-commerce presence impact audit risk and, consequently, audit cost?
   a. Audit risk increases, but not significantly
   b. Audit costs increases, but not significantly
3. Are the components of audit risk impacted by a material e-commerce presence?
   a. Moderate increase in all inherent, control, and detection risk
4. Does the amount of experience of the auditor, in the e-commerce environment, impact perceptions of changes in audit risk?
   a. Perception is dependent on the level of experience
The study suggests that CPA perceive audit risk, as well as its individual components, to be increased overall when it comes to E-commerce. At the same time, a majority of auditors suggested that audit costs would increase, suggesting changes in audit practice. These costs relate to changes in procedures, changes in scope, changes in timing of procedures, or some combination.
<table>
<thead>
<tr>
<th>Author</th>
<th>Title of Article</th>
<th>Periodical/Website</th>
<th>Vol./No./Edition</th>
<th>Year Published</th>
<th>Date Accessed</th>
<th>Location, Database, Website Link</th>
<th>Added to Final Paper?</th>
</tr>
</thead>
<tbody>
<tr>
<td>T. Burr, M. Gandara, and K. Robinson</td>
<td>E-commerce: Auditing the Rage; Auditors at Morgan Stanley Share a Unique Control Framework Developed During the Dot-com Craze</td>
<td>CBS Interactive</td>
<td></td>
<td>October 2002</td>
<td>June 1st, 2012</td>
<td>ca/daily-quotidien/111012/t11012a2-eng.htm</td>
<td>Yes</td>
</tr>
</tbody>
</table>