

Electronic Commerce Risks and Controls

Electronic commerce brings unprecedented flexibility in serving the taxpayers. It is quickly becoming a method of using a *public* network, the Internet, to transact and share information with anyone, anywhere. It's usefulness as a tool is exploding and the proof is in the numbers. In December 1994, there were only 3 million people using the Internet. Today that number stands at 140 million and is projected to grow to 56 percent of North American households by 2003, with as many as one billion users worldwide, by 2005.

Likewise, in the two years that the Internet has been used for commercial transactions, significant productivity gains are already being reported. As a recent Duke University survey found, it's no accident that two thirds of companies expect to purchase online in the year 2000, double the figure that bought online in 1998. The savings add up in personnel time, reduced document processing, and fewer errors. This explains why electronic commerce, *just* among businesses, is estimated to exceed \$300 billion by 2002. Clearly, the growth and benefits of commerce over the Internet continue to multiply and are here to stay.

We currently conduct business through computer systems contained and protected within state agencies. Electronic commerce means opening and integrating our core systems with the outside world. This obviously increases security risks. Yet the hidden risks are just as great. By instantly accepting information from environments, over which we have little knowledge or control, the problems of others can now quickly and directly become ours. Mounting statistics reveal the risks for those rushing to do business on-line.

For instance, the Federal Trade Commission has already issued 40 enforcement actions against misleading and deceptive online practices. In addition, a recent InformationWeek Online survey cites the following reasons for concern:

- Information loss has occurred at 22% of firms conducting Internet sales, compared to 13% of those not selling products on the Internet
- 49% of survey respondents did not know if they had monetary losses, due to security intrusions, last year
- For those respondents who *were* able to identify losses, due to security breaches, 84% estimate they lost between \$1,000 and \$100,000. The remaining 16% put losses at more than \$100,000

Surely, few of us would want to be included in the survey statistics above. Properly trained auditors can take the lead, ahead of the electronic commerce wave, anticipating the impact to audit trails, security, existing systems, and operating policies. By doing this, we can ensure that electronic commerce is not a liability, but just good, audited, and responsible business sense. To this end, the attached documents serve to identify specific risk and control categories, to help solidify state auditor leadership in successful electronic commerce.

Sources:

- U.S. Government Working Group on Electronic Commerce, First Annual Report, November 1998
- The Emerging Digital Economy, U.S. Department of Commerce, April 1998
- InformationWeek Online, Acceptable Risks, August 31, 1998
- The Digital Decade: Where Are Consumers Going?, Forrester Research, www.forrester.com, 1999

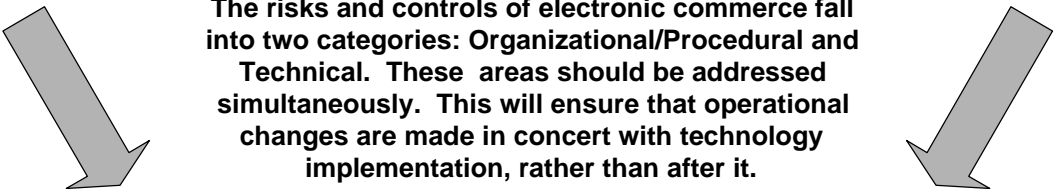
Electronic Commerce Risks and Controls - Overview

Organizational/Procedural Impact Items

1. Legislation
2. Procedures & Rules
3. Compatibility with Existing Systems
4. Audit Trail
5. Use of Organized Development Methods
6. Business Resumption Planning

Technical Impact Items

1. Security
2. Transmission Failures
3. Lack of Authentication
4. Security of Certificate Authorities
5. Internet Reliability and Year 2000 Readiness



The risks and controls of electronic commerce fall into two categories: Organizational/Procedural and Technical. These areas should be addressed simultaneously. This will ensure that operational changes are made in concert with technology implementation, rather than after it.



State
Agencies

Increased Electronic
Transactions and
Information Exchange

Public
Vendors
Agencies

Electronic Commerce
Risks & Controls

Below, there is an overview of electronic commerce related risks and internal controls. Some of these, such as those on legislation, apply to organizational and procedural changes. While others, such as those pertaining to computer security, apply to the technology itself and the changes needed to help make electronic commerce safe and successful.

TOPIC	RISKS	CONTROLS	EXAMPLES
Legislation	Without changes to legislation: <ul style="list-style-type: none"> State agencies may not be able to convert some key business processes to EC. The legal admissibility of EC transactions may also be in question. 	<ul style="list-style-type: none"> Identify legislative and business rule changes needed for successful EC implementation. Input from central rule-making agencies, such as a state comptroller or procurement agency, is critical. Participation from oversight agencies and those with statewide decision making authority. 	<ul style="list-style-type: none"> Legislation recognizing digital signatures (unique mathematical identifiers) as the equivalents of hand-written. Legislative changes may also be needed to allow agencies to do the following in computerized formats: accept formal documents; renew licenses; receive bids, etc.
Procedures & Rules	These risks arise from not modifying centrally administered rules and procedures governing the business process to which EC is applied.		<ul style="list-style-type: none"> Rulings requiring standardized automated procurement solicitation formats may be needed to consolidate solicitations on a state Internet site. Rules over processes such as delegated purchasing may need modification to ensure that EC can prudently be used for an optimum number of transactions.
Compatibility with Existing Systems	The data format for existing transactions may change when converted to EC. Difficulties could be encountered when integrating this data into existing systems.	As electronic commerce applications are identified, an impact analysis on an agency's current systems should be performed. In particular, interfaces between the EC system and current automated systems should be identified. This includes determining what type and format of information should be captured and processed. This will help ensure that EC transaction data can be successfully used to build-on, replace, or supplement the existing data for decision-making and record keeping purposes.	The maximum benefit from procurement cards can be obtained by planning for the use of automated billing data from the card issuer rather than manually re-entering the data from printed billing statements.

TOPIC	RISKS	CONTROLS	EXAMPLES
Audit Trail	Electronic commerce increases the exchange of data between organizations. The exchanged data may be used for critical agency transactions and decision-making. Audit trail risks occur because we cannot always rely on the internal controls of our business partners. Any of their inaccurate data and audit trail weaknesses becomes our risks.	<ul style="list-style-type: none"> • Agencies should seek to do monetary or mission-critical EC with business partners who have obtained a WebTrust or similar certification. Such certifications help establish that a business partner is legitimate and that their data is reliable and auditable. • Agency audit trails need be modified to include key elements from EC business partners. • Audit trail elements can also be obtained from EC related software and hardware tools, such as the agency's Internet security configuration. • Any modified audit trails should be tested for reliability and should include consideration for contingencies, for time periods when EC partner data may not readily be available. 	In using procurement cards, the card processor keeps the record of a transaction id, who made a purchase (card number), a transaction date, etc. This information would have traditionally been recorded and processed by the agency. Off-loading this to the card processor is a cost saving, but it increases agency reliance on the card processor's audit trail.
Use of Organized Development Methods	In the rush to provide EC services, agencies may not apply structured development methods in creating these applications. Agencies may expend resources that do not support an agency's mission.	As when developing traditional computer applications, agencies should apply formal development concepts to EC applications.	Agencies may spend money and time on Internet services that do not support the agency's mission and strategic plan. A formal development process would include having standards for making sure agency Internet pages and content are consistent and that only authorized information is placed on the Internet site. It also includes performing cost/benefit justifications prior to development.
Business Resumption Planning	As the use of EC expands, there is a risk of not being able to efficiently conduct business should a disruption in service occur.	Agencies will need to modify their business resumption plans to include important processes conducted via EC.	

TOPIC	RISKS	CONTROLS	EXAMPLES
Security	Unauthorized data accesses, modification, destruction, and the chance of accidentally disclosing confidential data.	<p>Organizations using EC, especially over the Internet, will need to adopt new layers of security.</p> <ul style="list-style-type: none"> • Security software and hardware to control access beyond publicly available information • Methods to ensure the confidentiality of transactions, as well as the authenticity of the transacting parties • Keys should be located on physically secured computers to prevent unauthorized use. <p>To compliment the new layer of security tools, agencies should formally establish how EC security is administered and monitored. Computer security policies should</p> <ul style="list-style-type: none"> • Ensure that Internet firewall security settings are reviewed periodically, • Reflect agency policy, and, • Ensure that security violations are identified and investigated in a timely manner. <p>The types of data access and transactions allowed via EC should adhere to a formal data confidentiality scheme adopted by each agency.</p>	<ul style="list-style-type: none"> • A firewall should be used to restrict, monitor, and provide an audit trail of access to an agency's Internet computer and to the rest of its computer network.
Transmission Failures	Unintentional errors, lost transactions, and duplication of transactions	<ul style="list-style-type: none"> • Electronic confirmations are sent or received. • Message sequence numbers can protect against message replay or reordering. The sequence numbers should be included in the message authentication check or encrypted to guarantee their integrity. • Hash or batch totals are used to verify completeness or accuracy of information. • EC errors are recorded, corrected, and reprocessed until correct. • Translation software checks for field formats and length. 	<ul style="list-style-type: none"> • EDI contracts typically include descriptions of controls to prevent loss of transactions. Auditors should review contract and determine if the agency is validating the information sent with batches of transactions to ensure that all transactions are received and processed.

TOPIC	RISKS	CONTROLS	EXAMPLES
Lack of Authentication	Electronic messages lack traditional identifiers and increase the risk that you may unintentionally deal with the wrong party, or deal with someone impersonating another party	<p>Message authentication providing the following:</p> <ul style="list-style-type: none"> • Positive identification of who is sending and receiving the message • Identification of where the message originated. This may clue someone in if the origin of the message is unknown, or does not match the sender's usual location. • Non-repudiation, ensuring that a party cannot later claim that they did not participate in a transaction • Assurance that the content of a message has not been changed <p>Message integrity is achieved by "sealing" a message or by "signing" a message.</p>	<ul style="list-style-type: none"> • Signing a message involves the generation of a digital signature • A digital signature is an electronic identifier intended by the person using it to have the same force and effect as the use of a manual signature. • Digital signatures are provided by a certificate authority, a trusted third party that usually contracts for these services.
Security of Certificate Authorities	<p>A certificate authority is a "trusted third party" who is responsible for ensuring that electronic parties are authentic. Risks associated with certificate authorities include:</p> <ul style="list-style-type: none"> • Trust in the user identification procedure • Strength of the key generation procedure • Security of the private key distribution process • Security of the public key certification and directory system • Availability of key recovery procedures 	<p>Legislation authorizing the use of a certificate authority typically requires that they undergo a SAS 70 review. At a minimum, the following controls should be in place:</p> <ul style="list-style-type: none"> • Identification of users should be documented and verifiable • Key generation procedures should be performed in a manner that there is no way for an outside party to recreate a user's key. • Strong encryption systems should be in place to ensure that the private keys, which identify an individual, cannot be intercepted, translated and used to impersonate the individual. • Certificate authorities should have strong security systems in place to protect the keys. • The certificate authority should have secure key recovery procedures in place, in the event that the individual cannot translate transactions due to a loss of the creating key. 	<p>For verifying the legitimacy of transacting parties and ensuring confidentiality, an agency should use a combination of security methods known as encryption and digital certificates.</p> <ul style="list-style-type: none"> • Together these tools mathematically scramble transactions and tag them with the identity of the author, in a unique manner. • The transactions can only be unscrambled with a specific, complimentary key. • Agencies should use a reputable source, known as a "certificate authority", to both issue their keys and verify the authenticity of transactions from others. This is similar in concept to how one's identity can be established by and verified through a reputable source, such as a national government, with a passport serving as the "key".

TOPIC	RISKS	CONTROLS	EXAMPLES
Internet Reliability and Year 2000 Readiness	Electronic commerce and specifically the Internet are experiencing growing pains and presents a reliability risk to agencies. Similar reliability risks occur because business partners may have Year 2000 bugs.	<ul style="list-style-type: none"> • Agencies should be aware of these reliability issues and enter into EC in stages where possible. • They should also evaluate which EC transactions are susceptible to Year 2000 problems, and ensure Year 2000 remediation is currently in progress. • To safeguard against Internet reliability problems organizations should have business continuity plans in place. 	<ul style="list-style-type: none"> • Some Internet vendors have experienced disruptions recently, and more may occur due to Year 2000 issues. • Business continuity plans will allow business to continue even if transactions through the Internet are not available.