

e-Commerce Security—Business Continuity Planning

Supported and authored by Deloitte & Touche, Information Systems Audit and Control Foundation,

ISACF Board of Trustees, ISACF Research Board 2002

Reviewed by: Linda M. Kinczkowski, Ph.D.

With the Internet increasingly becoming a part of everyday culture, it is imperative that organizations have a business continuity plan in place that includes e-business activities. Management needs to know and understand that information is a valuable asset and must be thoroughly protected, along with ensuring the ability to resume business operations should an incident occur.

E-security must be implemented for successful business resumption to occur, whether an incident is planned for or not.

This book provides a planning method that has been adapted to the requirements of e-commerce, as well as the necessary information to ensure that “protection and recovery of production resources” are continued and maintained.

This technical reference book allows for businesses and organizations to implement prescribed methodologies, which enables them to continue operations in the event of an interruption to the information systems that support their critical business processes. The book also provides information to help identify what impacts to business processes exist if an application or system becomes unavailable for an unacceptable period of time.

With e-security evolving from an IT infrastructure concern to a business concern, enterprises that can recover e-commerce capabilities rapidly, with minimal data loss and downtime, expand their reputation and are considered credible, ready and able, and resourceful. Organizations that do not take this seriously risk loss of revenue and possibly bankruptcy.

The authors examine “the typical business continuity planning model and highlight how the special requirements of e-commerce have shifted the emphasis.” The book’s design presents guidelines and templates, which are especially useful to the individual who is implementing business continuity planning in an e-commerce environment.

The book is organized in a manner that is easily understood. It covers the following areas with a strategic approach:

- Business continuity planning and evaluation
- Business assessment
- Strategy selection
- Plan development
- Testing and maintenance

The reference guide is enhanced further with the inclusion of an audit program and an internal control questionnaire, which is especially valuable with direct reference to COBIT® (*Control Objectives for Information and related Technology*).

The target audience for this book includes business managers, security and audit professionals, and educators and students who focus on information security and business continuity and/or disaster recovery planning, as well as others concerned with limiting risk.

This book is an extremely useful management tool for identifying the optimum, and most cost-effective, methods and controls. It is an excellent resource that not only provides planning techniques, but also the precautions and the procedures that organizations should use or apply since e-commerce is such a unique business component.



Editor’s Note:

e-Commerce Security—Business Continuity Planning is available now from the ISACA Bookstore. For information see the ISACA Bookstore Supplement in this *Journal*, visit www.isaca.org/bookstore, e-mail bookstore@isaca.org or telephone +1.847.253.1545, ext. 401.

Other guides in the *e-Commerce Security* series include:

- *Securing the Network Perimeter*
- *Public Key Infrastructure: Good Practices for Secure Communications*
- *Trading Partner Authentication, Registration and Enrollment*
- *A Global Status Report*
- *Enterprise Best Practices*

Linda M. Kinczkowski, Ph.D.

is the graduate program coordinator for the information security program at Eastern Michigan University (USA). She belongs to several associations including ISACA, ASIS, ISSA and ASLET.

Information Systems Control Journal, formerly the IS Audit & Control Journal, is published by the Information Systems Audit and Control Association, Inc.. Membership in the association, a voluntary organization of persons interested in information systems (IS) auditing, control and security, entitles one to receive an annual subscription to the Information Systems Control Journal.

Opinions expressed in the Information Systems Control Journal represent the views of the authors and advertisers. They may differ from policies and official statements of the Information Systems Audit and Control Association and/or the IT Governance Institute® and their committees, and from opinions endorsed by authors’ employers, or the editors of this Journal. Information Systems Control Journal does not attest to the originality of authors’ content.

© Copyright 2003 by Information Systems Audit and Control Association Inc., formerly the EDP Auditors Association. All rights reserved. ISCA™ Information Systems Control Association™

Instructors are permitted to photocopy isolated articles for noncommercial classroom use without fee. For other copying, reprint or republication, permission must be obtained in writing from the association. Where necessary, permission is granted by the copyright owners for those registered with the Copyright Clearance Center (CCC), 27 Congress St., Salem, Mass. 01970, to photocopy articles owned by the Information Systems Audit and Control Association Inc., for a flat fee of US \$2.50 per article plus 25¢ per page. Send payment to the CCC stating the ISSN (1526-7407), date, volume, and first and last page number of each article. Copying for other than personal use or internal reference, or of articles or columns not owned by the association without express permission of the association or the copyright owner is expressly prohibited.

www.isaca.org