Electronic Data Processing (EDP) Risk Control Checklist

Fire

- ☐ Provide portable halon substitute fire extinguishers
- ☐ Provide a separate EDP room when total values exceed $1 million dollars to include: walls, doors, etc., having at least a one-hour fire rated construction and protected by a fixed, automatic, total flooding extinguishing system
- ☐ Enforce a "No Smoking" policy in the computer area
- ☐ Use only Underwriters Laboratories (UL) listed waste cans
- ☐ Minimize storage of paper and other combustibles in and around equipment or software storage areas

Electrical

- ☐ Protect equipment from lightning strikes with a lightning arrester system
- ☐ When a storm is approaching, save your work and turn off the equipment, and if possible, disconnect the equipment from the power source
- ☐ Use only UL listed collateral equipment (power cords, power distribution units, phone cords, etc.)
- ☐ Install an uninterruptable power source (UPS)

Crime and Security

- ☐ Do not leave portable equipment in plain sight in parked vehicles
- ☐ Establish a policy and procedure for use of company approved software to help protect against computer viruses
- ☐ Control the physical access to EDP areas and equipment
- ☐ Have a security and fire detection system which is monitored by a central station under a service contract agreement
- ☐ Require passwords and that they be changed periodically, (recommend at least every two months)
- ☐ Install anti-virus software and keep it up-to-date
- ☐ Do not open attachments to e-mails generated from an unknown source
- ☐ Install software firewalls to protect your programs and data

General

- ☐ Place equipment where it is protected from hot and cold temperatures
- ☐ The computer room should be above the ground floor and in the center of the building
- ☐ Install independent HVAC systems in data centers to protect equipment from a high heat exposure
- ☐ Keep purchase records including the date, purchase price, description, and serial numbers of the equipment in a safe place (preferably off site)
- ☐ Maintain a copy of your software programs off site
- ☐ Back up computerized data/records on a disk at least weekly and store the disk off site
- ☐ Have a business resumption plan in place (refer to "Open for Business: A Disaster Planning Toolkit for the Small Business Owner" at www.IBHS.org)