Chapter 10: Risk Management and Control Procedures

TAKE CALCULATED **RISKS**. THAT IS QUITE DIFFERENT FROM BEING RASH.

George S. Patton (1885 1945)

WE ARE ALL **CONTROLLED** BY THE WORLD IN WHICH WE LIVE, AND PART OF THAT WORLD HAS BEEN AND WILL BE CONSTRUCTED BY MEN. THE QUESTION IS THIS: ARE WE TO BE **CONTROLLED** BY ACCIDENTS, BY TYRANTS, OR BY OURSELVES IN EFFECTIVE CULTURAL DESIGN?

B.F. Skinner (1904 - 1990)

Organizations considering cashflow reengineering are often concerned about the *business risks* in changing the patterns and procedures of their operations, some of which may have been in place for many years. A particular anxiety is that, in outsourcing activities to a vendor, there may be less focus than the company provides for the timely completion of important tasks. Managers fear that constituent groups, including customers, suppliers, creditors, employees and shareholders, may be negatively affected by reengineering initiatives.

Managers often fail to appreciate the extent of risk in normal business operations, due to the fact that much risk in inherent in any transaction. We simply do not see risk because it is everywhere, Categories of risk include the following:[1]

- *Trading partner, credit or payment finality risk*. The risk of a customer's failure to pay or that final credit for a payment will be withdrawn due to that party's actions. The management of this risk was discussed in Chapter 9.
- *Treasury operation or fraud risk*. The risk of the theft or loss of funds, discussed throughout this chapter.
- *Bank settlement risk*. The risk that a bank handling your transactions will fail, discussed in Chapter 7.
- *Information risk*. The risk of the loss of data critical to the operation of your business, discussed in this chapter.
- *Financial risk*. The risk that the use of derivative financial instruments will result in large losses due to adverse moves in interest or currency exchange rates. Financial risk is discussed in the Appendix to this chapter.
- *Systemic risk*. The risk of the collapse of the payment system, possibly triggered by some cataclysmic event This risk is monitored by various U.S. and global government agencies..

[1]See R. Balaporia, V. Hruska and B. Pisapia, "Payables and Receivables: Keeping Risk Down as Technology Options Soar," *TMA Journal*, September-October 1994, pages 20-28, for a discussion of procedures at Pacific Telesis and Occidental Petroleum.

The explicit definition and categorization of risk is a necessary step in its effective management. The advantage of reengineering is that activities are under the proverbial "microscope" of management on an constant basis, rather than assumed as satisfactory or ignored in the absence of reengineering. In fact, this is effectively the essence of Principle X, discussed in Chapter 3, in that the job of management is the continual exploration of opportunities to improve the performance of the organization. This chapter discusses the primary business risks of cashflow activities: the risk of fraud and information risks. The management of these risks is reviewed by actions internal to the organization and through outsourcing.

Risk and Cashflow Reengineering

Business risk is pervasive because management's use of the scarce factors of production, land, labor and capital may result in a lesser return than would have been received if those factors were otherwise employed. The only rational way to deal with such risk is to analyze alternative courses of action continuously, and to select that action with the greatest return for an acceptable level of risk. If the risk-return relationship from a particular strategy changes, management must adjust its decision accordingly.

For example, a reengineering strategy may be to outsource the collection of receipts to a bank for

comprehensive processing; see the discussion in Chapter 6. The decision may be based on economics, in that the bid price may be below the cost of internal processing; it may be based on service and quality issues, in that the bank may offer superior service to that available internally; or it may result from other factors.

The manager would constantly monitor the performance of the bank to determine that the quality, service and price are as promised. Should any important factors deteriorate, the manager would be justified in pursuing corrective steps, possibly including terminating the service. Such remedies should be stated in the original contract or purchase agreement between the bank and the corporation.

Managers may well wonder as to the logic of outsourcing a function if such constant scrutiny is required, given the concern for offending any constituent group by a performance failure. However, business risk is always present regardless of whether an activity is conducted internally or externally, and the job of the manager is to monitor risk and manage it on behalf of the organization.

The Risk of Fraud: Internal Actions

Risk is integral to the responsibilities of the Treasurer, the position in a business designated to safeguard its cash and other assets. However, every manager with responsibility for cashflow

elements must be cognizant of the various risks related to those activities, and must be prepared to take action to manage the risks along with other organizational tasks. A primary cashflow risk is fraud, with an estimated 500 million checks are forged annually causing total losses in the billions of dollars.

The potential for check fraud has been increased recently with the issuance of the Federal Reserve Board's Regulation CC, requiring banks to grant access to deposits in two days for checks drawn on local banks and five days for non-local items. These requirements have caused bad checks to be honored by banks in some cases before they can show up as return items.

Our consulting engagements frequently uncover incidents of fraud and theft. For example, an insurance company issued a check in settlement of a claim for $70. It was altered to $70,000 using desk-top publishing technology, presented and cleared through the banking system, and not found by accounting clerks until three months had passed. When attempts were made to contact the depositor of the check, he had disappeared, to no one's surprise.

Fraud can be prevented by various initiatives internal to the organization. The material which follows discusses paper transactions and electronic transactions, as does the subsequent section on outsourcing.

Consider these *internal actions* to manage paper transaction fraud:

VERIFY THE VENDORS USED FOR PURCHASING. Fraud often occurs through the payment of invoices to phoney vendors and/or vendors who overcharge for their products and services. Every vendor should be paid off an approved list, maintained and changed by a senior manager totally independent of the payables and disbursement functions. Exceptions should be rare, and should require multiple approvals. Verification of the legitimacy of a vendor can be through any of the following:

- Require the vendor to provide a Federal tax identification number
- Conduct a credit check on the vendor with a credit agency
- Request some basic financial data, preferably obtaining an audited statement
- Visit the new vendor's premises
- Ask the vendor for names of corporate customers, and call those businesses both to determine quality of service and legitimacy

USE BLANK CHECK STOCK OR SAFETY PAPER. Companies often order up to a six months supply of pre-printed check stock. This inventory, possibly tens of thousands of checks, is stored in a warehouse area with current requirements sent to the check printing site, often a computer facility. Once those boxes of printed checks are placed in their holding bins, it becomes impossible to protect against theft.

It is a relatively simple matter for anyone with access to the check printing or storage area to steal several checks from the middle or bottom of a box of checks, and months may pass before anyone is aware of the theft. Inexpensive laser technology allows the entire check face, including the magnetic ink character recognition (or MICR) line to be printed on blank paper. Alternatively, use safety or watermark paper, made from multiple layers of colored fibers, to cause scarring or bleeding when erased or chemically altered.

SECURE SIGNATURE PLATES. Due to the number of checks produced by businesses, a signature plate may be used to "sign" each check. Many companies fail to protect signature plates when not in use, leaving them on the check signing machine during business hours or in a known, unlocked drawer. Signature plates should be secured in a locked facility when not in use. Whenever possible, wet (ink) sign checks, particularly those over a predetermined minimum (such as $1,000), and so indicate that requirement to the drawee bank and on the check face.

ELIMINATE CHECK SIGNING BY SIGNATURE PLATE. Either use printed letter for the signature, surrounded by such unique characters as Greek letters or typographical marks, or scan the signature by computer scanner onto the laser-printed check. Scanned signatures can be printed using various color combinations to make it more difficult to copy. By eliminating the check signing process, the potential for fraudulent signature plate is eliminated.

LIMIT THE NUMBER OF AUTHORIZED SIGNERS. Large corporations may have hundreds of authorized check signers on file with the bank, resulting from branch and other dispersed locations which often "require" signers for locally issued checks. A bank cannot verify checks signed by hundreds of different managers, and will simply honor any check presented. Furthermore, organizations usually fail to delete authorized signers from bank signature cards, even though they may have departed years earlier. Carefully monitor the list of authorized signers, and notify the bank as soon as a change occurs on that list.

ELIMINATE CHECK SIGNING BY SIGNATURE PLATE. Either use printed letters for the signature on the check, surrounded by unique characters (*e.g.*, Greek letters, typography marks) or scan the signature into the signature line. Scanned signatures frequently are reproduced using various color combinations to make copying difficult. By eliminating the signing process, the potential for fraudulent use of a signature plate is eliminated.

CENTRALIZE CHECK ISSUANCE. Avoid the opening of bank accounts at each facility of your organization for convenience, check encashment (cashing employee checks), or other reasons. All checks should be issued from one site under the management of a designated manager. Consider outsourcing the disbursement function to a bank or vendor by a daily transmission of your payables file, as discussed in Chapter 8. The bank/vendor will convert each payment to the appropriate form (check, ACH, EDI, wire transfer) and handle all movement of funds with the accompanying remittance advice.

WORK WITH LOCAL BANKS TO PREVENT PAYROLL CHECK FRAUD. A major source of fraud is the cashing of counterfeit payroll checks on a city's large employer, either at local banks or at other popular check cashing establishments (*e.g.*, liquor stores). Local businesses should receive information as to identification cards issued to employees, including the position of the photograph, the color of the printing and the background, whether a fingerprint is on the card, etc. Similar information should be provided regarding company check stock. Furthermore, a telephone contact should be provided if there are questions regarding whether an employee or a check is legitimate.

SECURE OVER-THE-WINDOW DEPOSITS. The physical delivery of a deposit of checks to the bank invites theft either by the employee or by an outsider. If you must have employees handle the deposit, have them bonded and require the reconciliation of the encoded and stamped bank deposit ticket with totals calculated from daily receipt processing. Be sure to alter the pattern of the trip to the bank, using different routes, going at varying times, and carrying the deposit in different bags or satchels. Don't let the trip be predictable to a waiting thief!

SECURE ACCESS TO AREAS WHERE SENSITIVE OR VALUABLE ASSETS ARE MAINTAINED, such as Treasury, Information Systems, Payroll or Accounts Payable. Access to Treasury may permit the theft of check stock and unauthorized use of your bank information reporting systems to do a fraudulent wire transfer. Access to other business areas may permit the tampering with internal systems to issue checks to phoney vendors or for payroll.

SEPARATE TREASURY AND ACCOUNTING RESPONSIBILITIES. Smaller organizations frequently have the same individuals open mail, deposit checks, apply cash to open receivables, pay vendors and issue checks. This is becoming particularly prevalent as organizations downsize. With fewer employees verifying each other's activities, there are numerous opportunities for fraud and theft. The best prevention is to force the separation of those duties, and to require at least two different employees to handle the receipt and disbursement of cash.

Electronic Transactions

This section addresses electronic fraud involving wire transfers, ACH transfers, and EDI transactions. Wires are final, same day transfers. Once they're sent from your treasury shop, they are gone. ACH transfers are uniform next day settlement, and EDI transactions are value dated, allowing the transaction to be released on the date specified by the originator. Therefore, some opportunity is provided for the stop and recall of ACHs and EDIs after the transaction has been released.

Because of the finality of wires, most security has been directed toward protection of that process, with much less concern for ACH and EDI. For example, most wire systems contain multiple levels of security, including initiation, verification and release.

Furthermore, ACH/EDI transfers were, until recently, a largely "closed loop", in that mainframe computer systems were required to create ACH transaction tapes, which were then couriered or data transmitted to the bank. Today, numerous banks offer personal computer terminal-based ACH/EDI capability, which offers flexibility to the user but vastly increases the opportunity for fraud.

ESTABLISH PHYSICAL CONTROLS FOR THE COMPUTERS USED FOR WIRES AND ACH/EDI TRANSFERS. Do not allow any more access to these terminals than you would to pre-printed check stock. Secure the terminals to their desks by locking devices; restrict access to the work area where the equipment is housed; and provide lock-and-key safety for backup copies of tapes and disks supporting the money transfer systems.

USE ACCESS CODES WITH YOUR TREASURY SYSTEMS. Secure passwords (if used), and require a minimum of 6 frequently changed characters. Do not allow passwords to be shared or to be posted in accessible areas. Do not allow unlimited attempts to sign-on. If you do, a computer hacker will eventually discover your password. Instead, allow three tries, after which the user is logged off and access is forbidden.

CONSIDER PROHIBITING TELEPHONE OR OTHER MANUAL WIRES, due to the significant opportunity for fraud. Establish repetitive wire transfers whenever possible, designating specific accounts and codes involved in the transfer. If manual wires must be used, limit usage to funds movement between bank accounts. Do not allow facsimile (fax) signature authority for

electronic transactions, as a legitimate signature could be pasted onto a fraudulent transfer request. Insist on "wet" (ink signed) signature approvals.

ESTABLISH A SECURITY ADMINISTRATOR TO MANAGE USER ACCESS. The responsibilities of a security administrator would include issuing/changing user identification codes, receiving test material, handling changes to the system as initiated by the bank or by you, assigning transaction limitations, etc. To maintain a complete separation of functions, the security administrator should not have transaction authority to the payment systems.

REVIEW ALL PROCEDURES RELATED TO THE TRANSMISSION OR DELIVERY OF DATA TAPES OR DISKS. To prevent fraudulent media from being substituted for the original documents, require all movement to be in locked bags. Do not allow a delivery person to have access to the bag.

The Risk of Fraud: Outsourcing

Banks and vendors of financial services are expert at managing the risk of fraud, given their vast experience with the requirements of their own organizations. Most outsourcing products cannot be provided by companies at or even near the level of expertise, given the significant fixed costs and technology required. These outsourcing actions can help to manage paper transaction fraud:

For Paper Transactions:

USE OF POSITIVE (MATCH) PAY. Positive or match pay is a *daily* reconciliation product, as compared to the *monthly* full account reconciliation described in Chapter 8. It involves the transmission of an organization's issued check file to the bank, including check number and amount. As items are deposited and returned through the banking system and presented for clearing, any item where there is not a match of either factor is referred to the issuer for approval or rejection. The issuer normally has about one-half a business day to make this decision. This product prevents the honoring of checks pulled fraudulently from the bottom of a stack of pre-printed checks, and checks altered after issuance.

Positive pay works when checks are deposited and clear through the banking system for credit to the depositor's account. If a fraudulent check is cashed, as might occur with a payroll check, positive pay will not prevent a loss to the bank and/or to the corporate issuer. Desktop technology has created the opportunity for forgerers to scan a corporate logo and an executive signature from an annual report or other public document.

The company's bank account data may be obtained from various sources, including contacting the company and asking for the bank account number on the excuse that money is to be wired in payment of an invoice. The phoney checks are cashed, often by gangs operating in a team on a single

community, who then leave town before the loss is discovered.[2]

In response to these frauds with payroll checks, companies are emphasizing direct deposit programs (see Chapter 8). Another strategy is to encourage banks to fingerprint or "triple identify" non-customers attempting to cash checks. (A triple identification involves proof of identity through a driver's license and two credit cards.)

OUTSOURCE THE HANDLING OF CHECKS RECEIVED TO A BANK LOCKBOX. Theft may occur when checks are received in an office and a deposit ticket is prepared. This is a particular problem if the same individuals have responsibility for cash management and cash application. Regardless of float issues, consider having a bank lockbox (discussed in Chapter 6) handle the entire transaction flow, with any check disappearance the liability of the bank.

SET LIMITS ON WIRES AND ACH/EDI TRANSFERS for each transaction, for files of transactions, and for settlement day totals. Determine if your bank has software which can review a set of transactions to determine if these limits are exceeded, so that you can be notified. Consider positive or match-pay systems, which provide receiving banks with lists of authorized transactions against which an ACH/EDI file is compared.

[2]See "Bank Fraud, The Old-Fashioned Way," *Business Week*, Sept. 4, 1995, page 96.

For Electronic Transactions:

CONSIDER ENCRYPTION AND AUTHENTICATION TECHNOLOGIES TO ENHANCE THE SECURITY OF ACH/EDI TRANSACTIONS. Encryption involves the scrambling of data into unreadable cipher. Authentication provides protection against the tampering of data by detecting any deletion, insertion or modification. Both technologies involve the use of algorithms and secret keys known only known to the company and the bank.

INVESTIGATE THE USE OF SMART CARDS which frequently revise access codes and require PINs (personal identification numbers), similar to ATM cards. This technology requires the card entries of these codes to be verified by the host computer, allowing transactions to proceed if matches occur for the ones expected at that exact time of day.

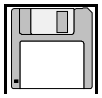
ENCOURAGE YOUR BANK TO USE ELECTRONIC CHECK PRESENTMENT (ECP) to speed notification of NSF or dishonored checks. There are two components to ECP: electronic cash letter presentment to your bank (versus the physical delivery of clearing items), and access to comprehensive electronic data bases of known bad check writers and closed accounts.

<u>The Management of Information Risk</u>

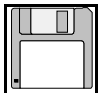
An often overlooked source of risk is *information risk*, that is, the risk of a loss of data critical to the operation of business activities. The dissemination of data throughout computing facilities and files makes regular back-up and protection difficult to control, and the proliferation of internal and external data sources adds significant complexity to this process. There is a large potential impact from a loss of proprietary business data.

There was a time not so long ago when all internal data was generated by a single mainframe system, making it a relatively simple matter to monitor access to the computer system to assure data integrity. Today, there are numerous internal data systems, including mainframe, minis and PCs, some stand-alone and some on LANs. External data used regularly by companies now includes bank information reporting, EDI feeds from VANs, on-line purchasing systems, the Internet, and various other types of interfaces.

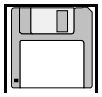
Exposure to hackers, viruses, accidents and intentional destruction has risen significantly, and few companies have developed procedures to deal with the resulting information risk. To protect your organization:



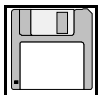
CAREFULLY REVIEW THE DISASTER RECOVERY PROGRAMS OF YOUR BANKS. Make certain that there are specific back-up and security procedures for data, that an alternative is available for processing in the event that the main site fails, and that a vendor has been contracted to provide further back-up in the event of a catastrophe.



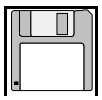
DEVELOP BACK-UP PROCEDURES FOR ALL INTERNAL COMPUTER SYSTEMS, including stand-alone and LAN (local area network) PCs. Don't forget laptop users! Create a secure library for all file back-ups, and make certain that every system is periodically represented using sign-in diaries or logs.



ANALYZE YOUR ORGANIZATION'S EMERGENCY PLANNING . Determine which tasks are essential for corporate survival, and develop procedures to accomplish those activities in the event that access is denied to offices or plant locations. Are the necessary files and equipment available to accomplish those tasks, and is an alternative office available?



PUBLISH A PROTECTION PLAN for your organization, distribute it to all affected managers and business units, and test it periodically to determine any flaws or oversights. Include in the plan such basic information as the home, automobile and beeper telephone numbers of key managers, and the critical tasks required to be performed to maintain the integrity of the organization.



REMEMBER THAT ELECTRONIC DATA HAVE VALUE AS BOTH A SOURCE OF FUNDS AND AS INFORMATION to a competitor or "reseller". Most controls are oriented to the protection of funds, while overlooking the possibility of the diversion of proprietary data for unethical uses. Protection must be developed for both sources of value, as well as for paper receipts and

disbursements. Your banks should be able to provide information on the security methods appropriate to the needs of your organization.

Using Policies to Manage Risk

The development and publication of policies and procedures on financial matters should supplement internal actions and outsourcing initiatives. Policies and procedures manuals are standard in specifying internal accounting rules, but only a small number of organizations have extended the process to other disciplines. Formal policies and procedures should be considered for various financial areas, as listed in Table 10-1.

Table 10-1: Cashflow Policies and Specific Topic Areas

General Policy and Rationale	Subject of Policy	Topics Covered by Policy
Liability Management:	Use of credit and debt	Monitoring of borrowings

to protect the credit rating of the business	capacity, including management of total commitments	Relationships with credit rating agencies Use of derivatives
Investment Management: to establish guidelines for the selection and custody of investments	Statement regarding appropriate investments, including levels of risk, maturities, criteria for investment firms handling securities, and other activities	Criteria of acceptable investments Securities lending Custody of securities Transaction processing standards
Bank Relations Management: to specify responsibilities for interface with banks	Statement regarding managers responsible for bank contacts, including the assignment of specific activities	Establishing bank relations Opening/closing accounts Signature authorizations Monitoring bank quality
Liquidity Management: to provide for adequate	Establishment of appropriate levels of working capital and	Cash collection procedures Cash concentration procedures

liquidity for the business	short-term cash	Cash disbursement procedures
Information Management: to limit the potential loss of important data	Establishment of procedures to safeguard and recover data critical to the mission of the business	Internal and vendor disaster recovery programs Systems backup procedures Emergency planning Control of access to proprietary data
International Transactions: to manage international transactions and funds	Establishment of guidelines to control the impact of currency fluctuations including exposure limits	Cash activities for international currencies Hedging currency risk International money transfer
Code of Conduct: to publish an ethics statement regarding employee behavior	Statement on employee conduct in accordance with legal and regulatory requirements and corporate policies	List of situations which are inappropriate, illegal or unethical; *e.g.*, soliciting gifts from vendors or customers, trading on insider information, nepotism, etc.

The publication of policies, and perhaps the specific procedures for each policy, can protect the organization from the activities of a foolish rogue or someone with evil intentions. The statement of acceptable levels of risk permit the periodic monitoring of compliance and the initiation of any necessary corrective actions.

Case: Managing the Risk of Derivatives

Managers have become alert to the risks from the losses on derivatives contracts, and some, like Gibson Greetings, Federal Paper Board and Orange County, CA, have major financial debacles on their hands.[3] Corporations and governments have been seriously harmed by betting on the direction of interest rates through the use of swaps, swaptions, other interest-rate contracts, and currency derivatives. A leading example is the dispute between Bankers Trust and Proctor & Gamble, the heart of which is whether the bank made oral representations as to the risk in the financing chosen to replace an expiring swap.

Derivatives are based on financial instruments, used fixed or floating rate debt (such as commercial paper or U.S. Treasury Bonds). A swap exchanges future cash flows between parties for a future period, such as fixed interest rate debt swapped for floating interest rates (or vice-versa). There are

[3]This is considered as financial risk, and is discussed more thoroughly in an Appendix to this chapter.

numerous variations of derivatives, including caps or limits on rates at which swaps are exercised.

According to published reports, Proctor & Gamble (P&G) was presented with three alternatives, one of which involved a wager on the direction of both short- and long-term interest rates. The company selected a swap based on yields on Five Year U.S. Treasury Notes and Thirty Year Treasury Bonds, even though internal valuations and the bank's pricing model were never disclosed. With the Federal Reserve boosting rates throughout 1994, the cost of terminating the swap rose over 14% above the interest rate on commercial paper, or a total of $195 million. P&G and Bankers Trust settled the matter before going to trial, with the bank accepting the largest share of the loss.

There were two mistakes made by the parties in this set of transactions. First, finance is always a staff function, not a profit center, and any transaction must support an inherent goal of the that function, such as reducing interest costs or exchanging fixed rate debt for floating rate. Finance should not be expected to make target transaction profits. Second, any financial transaction requires full disclosure of all pricing models and other elements which drive the deal's valuation.

Elements of a Policies and Procedures Statement

In order to prevent such problems, organizations should develop and issue policies regarding

appropriate behavior and acceptable risk. This approach is similar to policies developed by many treasurers regarding the opening of bank accounts, the execution of money transfers, and other sensitive matters, and involves:

- a statement as to acceptable practice
- levels of management permitted to commit the organization to specific levels of exposure
- penalties for violation of the policy
- responsibility for enforcement

Such policies should be distributed to internal staff *and* to investment and commercial bankers, with a signed copy retained by the issuer. Of course, there is no standard set of policies and procedures which apply to all organizations, because of the variance in the degree of risk acceptance; for example, some organizations will have a greater appetite for the use of derivatives than others.

For example, a policy on derivatives might state the following:

Rationale. Treasury supports the strategic business goals of the organization, and is not chartered to accept unreasonable financial risk.

Definitions of terms used: A derivative is a financial instrument which is derived from another, more basic financial instrument, with the value of the derivative based on that more elementary instrument.

Policy. No derivative contract may be executed which contains risk from the future direction of both short- and long-term interest rates, or involves a level of exposure greater than ½% point (50 bp) or other predetermined level ascertained by fully disclosed valuations.

Authority to Commit. The following managers are authorized to commit this organization to a derivative contract: the Treasurer or the Chief Financial Officer.

Penalties for Violation. Any employee found in violation of this policy is subject to immediate dismissal. Any bank or vendor involved in a transaction in violation of this policy will be barred from doing business with this organization for five years.

Enforcement. This policy will be enforced by Internal Audit staff, with advice from the Law Department.

While most organizations publish policies and procedures and distribute copies, employees too often have only a cursory knowledge of their content. Successful implementation -- and the avoidance of unacceptable financial risk -- requires that all parties sign a statement indicating that the policy has been read and understood. Furthermore, to assure adherence, there should be periodic independent audits of activities involving risk. The management of risk requires that organizational policies be established, that employees and vendors are aware of those policies, and that penalties are adequate

to assure compliance.

Triage for Business Risk

It is prudent to assume that your organization will be attacked by fraud, theft or system failure, or that a natural calamity, such as a flood or fire, will occur. You could be temporarily unable to conduct your normal business activities. Take steps now to assure that such a situation does not become a permanent closing!

The management of risk is a critical element in the life of an organization. Businesses and government have failed (or defaulted) because of a breakdown in the necessary surveillance of the various risks which can undermine corporate security. Certain internal actions are appropriate to mitigate risk; in other situations, outsourcing may be the appropriate choice.