Managing Cultural Assets from a Business Perspective

by Laura Price and Abby Smith

March 2000

Council on Library and Information Resources
Washington, D.C.

Published in Cooperation with the
Library of Congress

About the Authors

Laura Price is a senior manager in the Public Services–Assurance Practice of KPMG LLP in Washington D.C. Ms. Price provides audit and advisory services to Federal government clients in both the legislative and executive branches of the government. She worked closely with the Library of Congress in developing the business risk model described in this report.

Abby Smith is director of programs at the Council on Library and Information Resources (CLIR). Before joining CLIR in 1997, Ms. Smith was assistant to the associate librarian for library services at the Library of Congress. In this capacity, she worked with KPMG LLP to develop the business risk model.

ISBN 1-887334-75-0

Published in cooperation with the Library of Congress by:

Council on Library and Information Resources
1755 Massachusetts Avenue, NW, Suite 500
Washington, DC 20036

Web site at http://www.clir.org

Additional copies are available for $15.00 from the address noted above. Orders must be prepaid, with checks made payable to the Council on Library and Information Resources.

The paper in this publication meets the minimum requirements of the American National Standard for Information Sciences—Permanence of Paper for Printed Library Materials ANSI Z39.48-1984.

Contents

Figures and Tables

Preface

This report describes how the Library of Congress developed and implemented a plan for greater accountability over its collections. It is, in one sense, a case study. However, although the details of this study are unique to a single institution, the report sets out a model that can easily be adapted to every type of library, no matter how small, how specialized, or how atypical. The Library of Congress found itself in the awkward, if familiar, position of answering such questions from its oversight body as "How much are your collections worth?" "How do you determine how much to invest in security (or cataloging, or preservation, or collection development)?" and "What if you digitize your collections?" The business risk model described in this report was designed to help Library management answer these questions.

The role of collections and the funding it takes to make them productive are being called into question these days for several reasons. First, libraries no longer must have physical custody of an item—own it, in other words—to serve it to a patron. With the growth of interlibrary lending and the spread of networked resources, libraries have begun to uncouple collections and services. This development coincides with the increasing demand by funding organizations to manage library services and collections in a businesslike way. This notion is just as strange to libraries as was the notion of virtual collections 20 years ago.

Given how little data we have about the relationship between access to collections and the productivity of scholars, the achievements of students, or the general enlightenment of the public who use library resources, many managers are rightly concerned about treating the library business as a business. Nonetheless, it is not difficult to translate the work that goes on in libraries into the language of business. Nor is it incorrect to assess the effectiveness of libraries by investigating how responsibly staff members meet their obligations as custodians of collections. Responsible stewardship is at the heart of professional librarianship, and such stewardship is the focus of this report.

This report proposes a model that addresses the major challenges facing library managers, funders, and staff. Based on business risk assessment, the model defines library collections as core institutional assets and sets forth a model for accountability over those assets. It widens the definition of who is involved in the stewardship of library assets. Its aim is to guide managers in identifying both risk to collections and strategic investments in the productivity of institutional assets.

This report was developed with the cooperation of the Library of Congress through a partnership between the Council on Library and Information Resources (CLIR) and KPMG LLP, an international audit and business advisory firm. The Public Services–Assurance Practice of KPMG LLP developed the business risk model for the Library of Congress and coauthored this report with CLIR.

Abby Smith
Director of Programs

Introduction

Library collections are essential to providing the information services that patrons demand. Libraries acquire books, journals, films, prints, photographs, musical scores, maps, and manuscripts—regardless of genre or format—to meet the research needs of their present and future users. The collections, and the services that make these collections accessible, are essential to fulfilling the mission of a library. For research institutions such as university libraries, the collections often represent the accumulated capital of generations of scholars and creators (in many cases, faculty and former faculty) and constitute the raw material of future scholarship. For public libraries, the collections are the most tangible expression of the public trust that has been vested in them. The collections are the tools that libraries use to make information freely accessible to the citizens of the communities they serve.

Most libraries have traditionally focused more on the costs of acquiring and maintaining collections than on their potential as assets that are vital to institutional productivity. Without understanding the value of collections as assets to the home institution, however, it is difficult to determine how best to make those assets most productive. And without understanding risks to these assets, it is hard to protect them against future loss or damage.

This report presents a model for the management of library and archival collections that defines those collections as core assets and seeks to make them maximally productive while controlling risks to their integrity. The model is not based on the monetary value of library holdings. Instead, it focuses on business risk and proposes a framework of controls to minimize the risks that threaten the viability of those assets. This perspective views libraries as businesses and their collections as integral to achieving business objectives. With this model, managers can identify priorities for institutional investments in collections and make more compelling budget justifications for necessary resources, because the relationship between assets (collections) and the library's mission work is made explicit to financial decision makers. Although it may be evident that libraries cannot perform mission work without having the resources to ensure that collections are accessible and secure over time, it is not always evident which investments in collection development, preservation, and security will best serve the collections at a given time. This model is designed to help managers identify priorities for investment in these areas.

The business model offered here can help managers improve stewardship of their cultural assets because it defines and controls risk through a dynamic assessment process that incorporates the changing needs of library collections, services, and patrons. It is designed to apply not only to tangible assets, such as print collections, manuscript materials, or rare sound recordings, but also to intangible digital assets that today's libraries are acquiring and creating and for which they are equally responsible.

The fact that the language of this model comes from business, and accounting in particular, is indicative of the new environment in which all cultural institutions find themselves—one in which business increasingly sets standards for operations and accountability. Nonprofit organizations such as libraries and archives must compete for resources and make a strong case for continued or increased support for core activities. To obtain the necessary resources for mission work, library managers must be able to express and justify their needs in terms familiar to financial officers and funding organizations—in terms of business risk. The business risk model is easily adapted in library and archival environments (it is fully described in Appendix I). The body of the report discusses how the model can be applied in a library setting.

Business Risk in Libraries

Origins of the Risk-Assessment Model

The risk-assessment methodology described in this report has its origins in the efforts of the Library of Congress (the Library) to better manage its finances and strengthen its core business, that is, "to make its resources available and useful to Congress and the American people and to sustain and preserve a universal collection of knowledge and creativity for future generations" (Library of Congress 1997). Developed to be used in a working national library, the methodology is now an integral part of the Library's annual audit. Because the Library is an agency in the legislative branch of the Federal government, other libraries may not share its specific accounting requirements. Moreover, the scope and size of the Library's collections exceed those of other research libraries and, indeed, other national libraries. But the fundamental problems that the Library staff addressed with independent financial auditors from KPMG LLP as they developed the first-ever model to "account" for the well-being of heritage assets are the same as those facing any library—public or private, multimedia, or single-format.

The Library undertook its first audit in fiscal year 1995. For the purposes of this audit, the Library's collections were assessed not for their replacement value but for their cultural value. They were treated as "heritage assets," a term from the Federal Accounting Standards Advisory Board (FASAB)[1] Standard No. 6, *Accounting for Property, Plant, and Equipment*. The standard uses the term to define assets with historical or natural significance; cultural, educational, or artistic importance; or significant architectural characteristics. These assets are generally expected to be preserved indefinitely. Their monetary value may vary significantly from item to item; some items may even be irreplaceable. In all cases, the monetary value is seldom identical to the cultural value these assets provide for the communities they serve—past, present, and future.

The costs of acquiring, processing, and preserving collection items consume a significant portion of a library's annual budget. In Federal financial statements, the costs of keeping collections up-to-date, physically stable, and readily accessible are considered operating expenses in the period incurred. The heritage assets are quantified in terms of physical units (for example, number of items in the collections) and recorded in a supplemental schedule to the financial statements.

Although not required to do so by law, the Library of Congress elects to comply with laws to improve financial management in the executive branch agencies.[2] Each year the process begins with Library management making a statement about the adequacy of its internal controls over financial reporting and the safeguarding of its collections. ("Safeguarding" refers to the protection of the assets from theft, loss, or misuse.) The Library's independent auditors are required to express opinions not only on the fair presentation of the financial statements but also on whether management's assertions are accurate. In its financial statements for fiscal years 1995–1998, the Library was unable to assert that its controls over safeguarding of heritage assets were effective. The Library's auditors agreed with this assertion.

The Library could not assert that its controls were effective because the risks to its collections had never been assessed. A risk assessment is the foundation for establishing or improving existing controls in order to form an internal control framework that lets

[1] The FASAB was developed to standardize financial accounting in the federal government, and has as its coprincipals the secretary of the treasury, the director of the Office of Management and Budget (OMB), and the comptroller general of the United States.

[2] These laws include the Chief Financial Officer's Act of 1990 (CFO Act) and the Government Management Reform Act of 1994 (GMRA). These two acts provide for the preparation and audit of financial statements for executive branch agencies. The OMB prescribes the form and content of the federal financial statements under OMB Bulletin No. 97-01, *Form and Content of Agency Financial Statements*. The bulletin requires agencies that comply with the CFO Act to follow the accounting standards set forth by the FASAB. As a government entity, the Library adopts all accounting standards set forth by the FASAB and reports its financial statements in accordance with OMB Bulletin No. 97-01.

managers know the state of an organization's assets at any time. Absent that assessment, managers have only anecdotal feedback about the effectiveness of controls. While Library managers and staff had a fairly strong grasp of what threats existed to their collections and what actions could be taken to mitigate them, there were no data to support that knowledge or to demonstrate to funding organizations the need to invest in improving controls. To rectify this, the Library began systematically assessing the risks to its collections.

Defining Business Risk

To understand where its risks lie, management must be clear about what risks might threaten the mission of the institution. Missions vary widely among libraries and research institutions, as do their collections. For instance, the Library of Congress's mission is to "acquire, preserve, and make maximally accessible the intellectual and information heritage of the United States and, to the degree desirable, the world" (1997). The Library has many different types of collections with different levels of value, but the comprehensiveness of its collections is critical. Because the Library keeps items of research value indefinitely, it emphasizes collections care and long-term preservation.

Harvard College Library has a similarly ambitious mandate. Its mission statement says that it "supports the teaching and research activities of the Faculty of Arts and Sciences and the University. Beyond this primary responsibility, the Library serves, to the extent feasible, the larger scholarly community." In contrast, the mission of the Denver Public Library is "to help the people of [the] community achieve their full potential" by informing, educating, inspiring, and entertaining its patrons (2000). Although it does have special collections that are unique and rare, the Denver Public is not a library of last resort. Consequently, its acquisition policies, preservation and security measures, and circulation system differ dramatically from those of an institution that must serve a larger community over the course of centuries.

Libraries attached to scientific and technical institutes put a premium on currency of information and seldom have the same need for preserving collections indefinitely. The mission statement of the Caltech Library System declares that it "provides library resources and forward-looking information services of the highest quality in a timely, cost-effective manner to support and facilitate the research and educational programs of the Institute" (2000). For libraries such as those at Caltech, licensed access to databases, subscriptions to electronic journals, and heavy reliance on digital information (as opposed to historical literature) mean that robust information technology services may be more vital than the preservation of artifacts.

Just as the mission of a particular library determines the types of collections it builds and maintains, so, too, does mission set the course for creating the framework of controls that is designed to reduce its business risks. The Library's mission focuses on developing, preserving, and serving its vast collections. The first and fundamental step in identifying the chief risks to any of its collections, therefore, is to understand what threatens its fitness for use. What good would a book be if no one could use it, and what could happen to a book that would render it unusable? It could become embrittled and crumble. It could be misplaced, inadvertently through misshelving or deliberately through theft. It could be incorrectly cataloged and hence be unretrievable. These hazards are well-known to librarians, and much staff work goes toward reducing the chances that any of them will happen. To develop an internal control framework, librarians and their staff must be able to relate their daily activities to the corresponding policies and procedures under which they work. They must understand how the design of those policies and procedures reduces risks to the collections and be able to explain this framework to oversight bodies.

On the basis of its mission, the Library of Congress defined the following as important business risks:

1. The risk of not acquiring materials that are critical to the continued development of the research collections that meet the needs of Congress and the research community;

2. The risk of failing to make the collections available to users in a timely and appropriate fashion;

3. The risk of not preserving the collections from the physical degradation inherent in each of the various media the Library holds, and from deterioration through use; and

4. The risk of exposing the items in the collection to theft, mutilation, or accidental loss.

Risk-Assessment Process

Creating an Internal Control Framework

On the basis of its definition of business risk, the Library of Congress worked with its independent auditors to document substantial risks to the collections and to identify appropriate safeguarding controls. This process followed generally accepted standards for internal control developed by the Committee of Sponsoring Organizations of the Treadway Commission (COSO).[3] The COSO report on internal control, *Internal Control-Integrated Framework,* was written to establish a common language that business people, regulators, legislators, and others could use when communicating about internal control. It pro-

[3] COSO's oversight board consists of representatives from the American Institute of Certified Public Accountants, the American Accounting Association, the Institute of Internal Auditors, the Institute of Management Accountants, and the Financial Executives Institute.

vides a framework by which both public agencies and private sector businesses can understand their control systems. While this framework is widely accepted in the business and accounting communities, its terminology was new to the Library staff. By contrast, its concepts, which mapped closely to practices of responsible custody and service, were quite familiar to the professional staff.

The COSO defines internal control as “a process, effected by an entity’s board of directors, management and other personnel, designed to provide reasonable assurance regarding the achievement of objectives in the following categories: effectiveness and efficiency of operations; reliability of financial reporting; and compliance with applicable laws and regulations” (1991). The business risk model presented in this report was developed to satisfy the second of the five elements of the COSO framework, namely risk assessment. This element and the other four framework elements are as follows:

1. *Control Environment*. The control environment is an organization’s culture, beliefs, and values. It includes the integrity, ethical beliefs, and competencies of its people, which are visible in management’s operating style, how management assigns authority and responsibility, and how management organizes and develops its employees. Another indication of the control environment is the degree of involvement from its board or directors.

2. *Risk Assessment*. Risk assessment is the identification and analysis of internal and external risks relevant to the achievement of objectives. A risk assessment forms a basis for determining how risks should be managed. Assessments are a continuous part of the internal control process because emerging economic, regulatory, political, and operating conditions will change the type and degree of risks faced by an organization.

3. *Control Activities*. Control activities are the policies and procedures an organization develops to ensure that management’s directives are carried out and objectives are met. Control activities occur at all levels and in all functions within the organization.

4. *Information and Communication*. To conduct control activities and identify risks, mechanisms must exist within the organization to capture and communicate relevant information at all levels. Information systems produce reports with internal and external financial, operational, and compliance information that allows the organization to function. This information must flow up, down, and across the organization for the control environment to remain strong. External communication with customers, suppliers, regulators, and stakeholders must also be effective.

5. *Monitoring*. The internal control system must be monitored for effective performance over time and be evaluated periodically. Management and supervisors must constantly assess actions taken by

> staff in performing their duties. The frequency and depth of the monitoring activities depend on the amount and degree of risk faced by the organization. A successful monitoring activity is one that allows all serious matters to be reported to management in a timely manner.

The Library's auditors used this framework in fiscal years 1995 and 1996 to assess the status of the Library's safeguarding controls over its collections and to serve as a basis for the development of recommendations for improving those controls. The focus of the auditors' assessment was control activities, which in the Library range from cataloging standards and practices to protocols for the physical handling of acetate disks or eight-track tapes. Despite the absence of a baseline risk assessment for the collections, the auditors could draw significant conclusions about the control environment and note what information was gathered, how well it was communicated, and how various monitoring systems operated. How were managers held accountable for the collections in their custody? How was performance evaluated, how often was it done, and what authority did managers have to enforce policies that served to protect the collections? What orientation and training did the staff receive about workplace policies and procedures? What instructions were patrons given about proper handling procedures for rare or fragile materials? The control activities of an institution provide the answers to these questions.

Based on the results of the audits, the Library decided to conduct formal risk assessments of the environments and control activities within selected divisions. The assessments would be done in the divisions where collections of differing formats were either permanently stored or temporarily handled as they arrived, or where they were serviced in some manner within the Library. That way, staff could assess the risk to items over the course of their life cycle—from acquisition to cataloging and from service to storage. Staff could also distinguish between the risks to different types of material. For example, the risks to a recent monograph on the Japanese economy, printed on acid-free paper and of little artifactual value, would be different from the risks to a Hollywood feature film from 1956 or to the 1991 *Sports Illustrated* swimsuit issue. Each item has its own risks, based on physical features of the recording medium and perceived value, and in each case, the risks are dynamic and change over time. A judicious choice of formats and genres produces a risk assessment that allows extrapolation from these data to similar types of collection items.

Library management realized that risks would need to be calibrated on the basis of the likelihood of their occurrence and on the magnitude of impact, should they occur. The Library's safeguarding risk, i.e., the risk of not controlling what happens to the overall condition of the collections, was defined as follows:

> The risk associated with an internal control weakness over the safeguarding of the collection assets is assessed as *high,*

moderate, or *low,* depending upon the degree to which present policies and procedures make it highly probable that:

1. The Library will incur a loss of collection items (by theft, damage or misplacement), and the loss will not be detected in a timely manner by personnel in the ordinary course of business;
2. The Library will not be able to serve the needs of Congress, the U.S. government, or the public through service or accessibility to the collection assets;
3. The Library will not be able to acquire materials critical to the continued development of the research collections; and / or
4. Management will not receive enough information to determine whether its objectives, with respect to collection assets, are being achieved.

Whether risk was acceptable would be determined by the degree to which one or more of the above situations could occur (likelihood of occurrence) and the degree to which the situation would adversely affect the integrity of the collections (magnitude of impact). These situations may occur because of the absence of an effective policy or procedure, or failure to adhere to the policy or procedure. For example, moving materials from a custodial division to the preservation department without creating any paperwork to document the transfer would be one such unacceptable practice. This could occur either because there was no policy regarding paper documentation in place or because the staff ignored the policy. Creating and enforcing such a policy would greatly reduce the risk of theft, loss, or misplacement of Library materials.

Identifying Relevant Controls

Before the Library could begin its risk assessment, management had to determine which internal controls were relevant. Just as the clues to uncovering business risk are found in the mission statement, relevant controls are derived from an examination of business risks. For example, from the four salient types of risk the Library identified, it derived four corresponding types of “safeguarding controls” that mitigate those risks to its collections. They include *bibliographic, inventory, preservation*, and *physical security* controls.

Given the many formats that the Library holds and the complexities of controlling them both physically and intellectually, controls vary among formats and media. The degree and type of control placed on an item depend upon its relative value and risk of loss or deterioration relative to other items in the collection. The demand for and condition of an item may vary. Nonetheless, whether the item is a videotape, a Thomas Jefferson holograph letter, or an illustrated elephant folio from 1750, it must have bibliographical control, be retrievable through some inventory or tracking system, be protected from physical degradation or loss of information content, and be secured from theft and mutilation.

Table 1, on pp. 10–11, defines the Library's four relevant controls, provides examples of each type, and describes risks that may be present if these controls are weak. While not all libraries will face the same risks in equal measure and degree, the risks they face will fall into these four categories, as will the controls designed to mitigate them.

Determining How to Assess Risk

The Library separated its collections by format before attempting to assess risk. This was done for several reasons. First, only about one-quarter of the Library's collections are books and serials. Most are special collections. Whereas the book collections are housed in centrally controlled storage areas and from there served in several reading rooms, the special collections are separately housed and controlled and served in separate reading rooms to researchers.[4] For instance, music scores are housed and served in the Music Division, whereas maps and globes are housed and served in the Geography & Map Division. Within each special collection division, items also have different formats. For example, recorded sound may be kept on LPs, CDs, cassettes, or other media.

Second, the degree of risk will vary, depending upon the format of the item. A single-page manuscript has a higher risk of physical loss than does a large monograph. Therefore, the risk-assessment process would be more efficient if collections were first segregated by major format types that tend to share similar risk.

To establish a common language for this segregation by risk, the Library uses names of five precious metals—platinum, gold, silver, bronze, and copper—that describe groups of items in the collections by degree of tolerance for risk. The Library defined each group as follows:

Platinum includes the Library's most priceless items. The *Treasures*, a small group of the Library's most precious items, such as the Gutenberg Bible, are the quintessential components of this category.

Gold includes rare items that have prohibitive replacement cost, high market value, and significant cultural, historical, or artifactual importance. This includes first editions and rare books, daguerreotypes, manuscript maps, and wax cylinder recordings.

Silver includes items that require special handling and items at particularly high risk of theft, such as computer software, popular titles in print, videos, and compact discs.

Bronze includes items served without special restrictions in the Library's reading rooms and materials that may be loaned without stringent restrictions.

[4] Some special format collections share off-site storage space, but this is undesirable and has been assessed as a risk to the inventory control and preservation of those items.

1. Bibliographic Control

“What do we have?”

Examples of Activities	Potential Risks from Weak Control Activities
• Cataloging • Archival processing • Reducing cataloging and processing backlogs	An institution may store a significant number of unprocessed or uncataloged items. Such items may be inventoried but not yet recorded in a publicly accessible catalog or finding aid, so researchers do not know the items are available for use. A librarian or library technician would have to know the unprocessed items exist and know where to find them in order to serve them to researchers.

3. Preservation Control

“How can collection items be protected from physical loss or damage due to improper handling or storage?”

Examples of Activities	Potential Risks from Weak Control Activities
• Serving surrogates (digital, microform, reference copies of audiovisual materials)	Original works may become inaccessible because their format cannot be restored and no measures have been taken to reproduce them in a more stable medium.
• Programs for collections care	Monographs produced on acidic paper may deteriorate if they are not deacidfied.
• Preservation treatment of processed items	Items that require preservation treatment may not be identified because the institution does not have a program to identify them in a timely manner.
• Planning for proper storage (adequate space and appropriate environment)	Temperature and humidity controls within the collection storage areas are inadequate to properly preserve the stored items. Storage space is insufficient to meet current or future needs. Stored items may suffer damage because there is insufficient shelf space or a lack of space for protective housing.

Table 1. Relevant controls for potential risks

2. Inventory Control

"Where are the items located?"

Examples of Activities	Potential Risks from Weak Control Activities
• Automated circulation control systems	The existence of collection items may not be recorded (inventoried) by the institution when the items are received. Without a record of existence, even the library staff will not know about them. The staff will also not know if items are lost or stolen. If items must travel among many departments of the institution for cataloging, treatment, and storage, or to an off-site location for service or storage, and the movement of the items is not tracked, the institution may have no way of knowing where to locate the items.
• Shelf lists	A shelf list may be in manual form only, preventing it from being easily updated.

4. Physical Security Control

"How can collections be protected from physical loss or damage due to improper handling or storage?"

Examples of Activities	Potential Risks from Weak Control Activities
• Engaging building perimeter security, including exit inspections and theft-detection devices	Valuable research or collection items are not equipped with theft-detection targets or other methods for identifying when someone is attempting to remove them from the premises. The institution's buildings that house valuable research or collection items have no physical deterrents to prevent vehicles with bombs from approaching or other terrorist actions from occurring.
• Closing stack access to the public	An institution has no physical security to ensure valuable research items or collections cannot be removed.
• Registering readers	An institution has no record of its readers' identities or addresses, making it impossible to locate them in the event an item they were using cannot be located.
• Restricting loans to authorized organizations or individuals and documenting the transaction	An institution with no formal loan policy for its materials has no recourse in the event an item is lost or damaged by an organization to which it was loaned.

Copper includes items the Library does not intend to retain but holds while deciding; for example, items that may be used for its exchange and gift programs.

Other libraries can readily devise similar ranking systems to define degrees of risk specific to their collections.

This risk tolerance category determines the levels of controls placed over the Library's items. Manuscripts usually consist of unbound sheets of paper, such as letters. Because these sheets can be easily lost or misplaced and because it is seldom cost-efficient to institute item-level bibliographic and inventory control over manuscript leaves, physical controls are put in place to compensate for this situation. Such controls must be strong in areas where the items are likely to become lost, stolen, or damaged, such as in the reading room. Additional security personnel may be required to monitor researchers' actions, and researchers' activities may be limited; for example, they may not be allowed to bring personal items into the reading room. These are difficult trade-offs for both library staff and researchers. Libraries that require their readers to modify their behavior to protect the collections must make it clear to their patrons why the measures are deemed necessary.[5]

The Library of Congress, as a library of last resort that serves primarily the research needs of Congress, has a low tolerance of risk for monographs and manuscripts. In the past decade, the Library has greatly enhanced security and restricted access to its general-collections stacks. But not all libraries have closed stacks, even if it places their collections at some risk. In some cases, the measures of protection afforded by physical security are provided in other ways. College libraries, for example, usually have open access to their stacks and so must institute policies and procedures that mitigate the havoc that can result when students pull books from the shelves and incorrectly reshelve them, or take them to the dormitory without checking them out. College library managers may accept the risk to their collections when those controls fail occasionally, because it is worth it to meet student needs.

To provide examples of how control environments differ among different collection formats at the Library, Table 2 on pp. 14–15 compares and contrasts the principal safeguarding controls of three types of collections: monographs, manuscripts, and prints and photographs.

Controls vary with the format of the material, because each format resides in a different environment and is subject to different types of handling. These differences are apparent in the physical control risk category. If lost or stolen, some monographs can be readily replaced, while others cannot. These differences affect the amount of risk to the assets that management is willing to tolerate. Management

[5] To avoid inconveniencing patrons, managers often resist simple security and preservation controls that greatly reduce risk to the collections, such as requiring researchers to don protective gloves to examine fragile materials or allowing only staff to photocopy materials. Simple explanations of why a certain practice is good stewardship—on the patron's part as well as the library's—obviates complaints in most cases.

has less risk tolerance for items of considerable value that cannot be replaced than for those items that can be bought in the marketplace.

Conducting the Risk Assessment

In 1997, the Library chose to start the risk assessment process by examining its Geography & Map Division. The collections in this division, while all containing geographical information, are recorded on diverse media, from vellum to computer disk. The highly diverse formats of geographical information, including atlases, globes, and single sheet maps, have a variety of bibliographical and preservation needs. In addition, and unlike many other divisions, the primary processes of creating the inventory, bibliographical, preservation, and physical security controls all take place within one physically integrated, purpose-built space. These considerations, together with a highly knowledgeable and experienced staff, made this particular collection an ideal place to begin the process of translating library practice into a business model.

A team of KPMG consultants and Library managers performed the risk assessments. KPMG provided the structure for the risk assessments, employing internal control evaluation techniques similar to those used for financial statement audits. The process was performed separately for each participating division. Figure 1 on page 16 depicts the procedures that made up the risk assessment process.

Step 1: Define Risk. The risk assessment started with defining risk. This definition served as the measure against which business risks were compared. From this comparison, management determined whether business risks were acceptable or whether controls needed to be instituted to mitigate some of them.

Step 2: Conduct Interviews and Walk-Throughs. Together, KPMG and Library managers walked through each division to understand and document the general flow of materials within the division. The walk-through was repeated if different types of formats moved about in different ways.

Step 3: Document the Control Environment. Based on the interviews and walk-throughs, the team prepared a memorandum that documented the flow of materials in the division. The memo began by describing how the materials entered the division. It described the processes used to accession, catalog, and prepare the items for use. The documentation concluded by describing whether the items were stored within the division or sent to other areas of the Library. The documentation included examples of manual or computer-generated forms the division used to track and control the movement of items. A flowchart was prepared to illustrate the movement of materials.

Step 4: Define the Key Controls. Using the documentation describing the control environment, the team identified and documented the important internal controls that were in place and functioning in each process.

Step 5: Define the Control Weaknesses. From the documentation prepared in Step 3, the team identified and documented weaknesses

1. Bibliographic Risk

An item may not be usable because the user cannot locate a record of its existence, by title, author or subject.

Monographs	Manuscripts	Prints and Photographs
Bibliographic records are kept in an electronic database. System backups are performed regularly.	Bibliographic records may be maintained at a group or collection level, in a system where backups are performed regularly.	Similar control as manuscripts.

3. Preservation Risk

Items may not be usable because they are too fragile.

Monographs	Manuscripts	Prints and Photographs
Inspections are conducted of valuable items to detect damage or deterioration.	Similar control as monographs.	Similar control as monographs.
Surrogates, such as microfilmed copies, are served to researchers so originals can be handled sparingly.	Fragile items are copied onto acid-free paper during preparation for storage.	Surrogates, such as digital images and copy prints, are served when originals are fragile.
Temperature controls and hydrothermographs are used to monitor the physical environment of the stacks.	Similar control as monographs.	Similar control as monographs.
Signs are posted in reading rooms instructing patrons on how to handle books.	Similar control as monographs.	Similar control as monographs.

Table 2. Key safeguarding controls in three collections

2. Inventory Risk

Items cannot be located because their location is not recorded.

Monographs	Manuscripts	Prints and Photographs
An accurate and fully functional shelf list is maintained to locate items not on the shelf, checked out, or on loan.	Comprehensive shelf lists may be impractical for institutions that house large numbers of manuscripts. Physical controls must compensate for lower degrees of inventory control.	Comprehensive shelf lists may be impractical for large numbers of individual photographs that may by grouped by subject or photographer. Physical controls must compensate for lower degrees of inventory control.

4. Physical Risk

Items are subject to loss or misappropriation.

Monographs	Manuscripts	Prints and Photographs
Stack areas are off limits to the general public.	Similar control as monographs.	Some items are available for general use in the reading room. Patrons can select these items on their own. Service of this nature is limited to less valuable items.
Items of special interest or extraordinary value are placed in locked areas, with restricted key access.	Manuscripts are inherently susceptible to loss or misplacement. Additional security in the reading rooms is necessary to discourage theft because segregation of valuable and invaluable items is difficult.	More valuable or fragile items are kept in stacks that are not accessible by the public.
Security cameras are placed in reading rooms and study areas.	Similar control as monographs.	Similar control as monographs.
Access to other areas of the building is limited to employees.	Similar control as monographs.	Similar control as monographs.
Books are tagged with electronic devices that activate an alarm at a library exit gate if an attempt is made to remove them from the premises.	Researchers are restricted from bringing personal belongings into the reading room. Manuscripts cannot be hidden in personal belongings.	Similar control as Manuscripts.

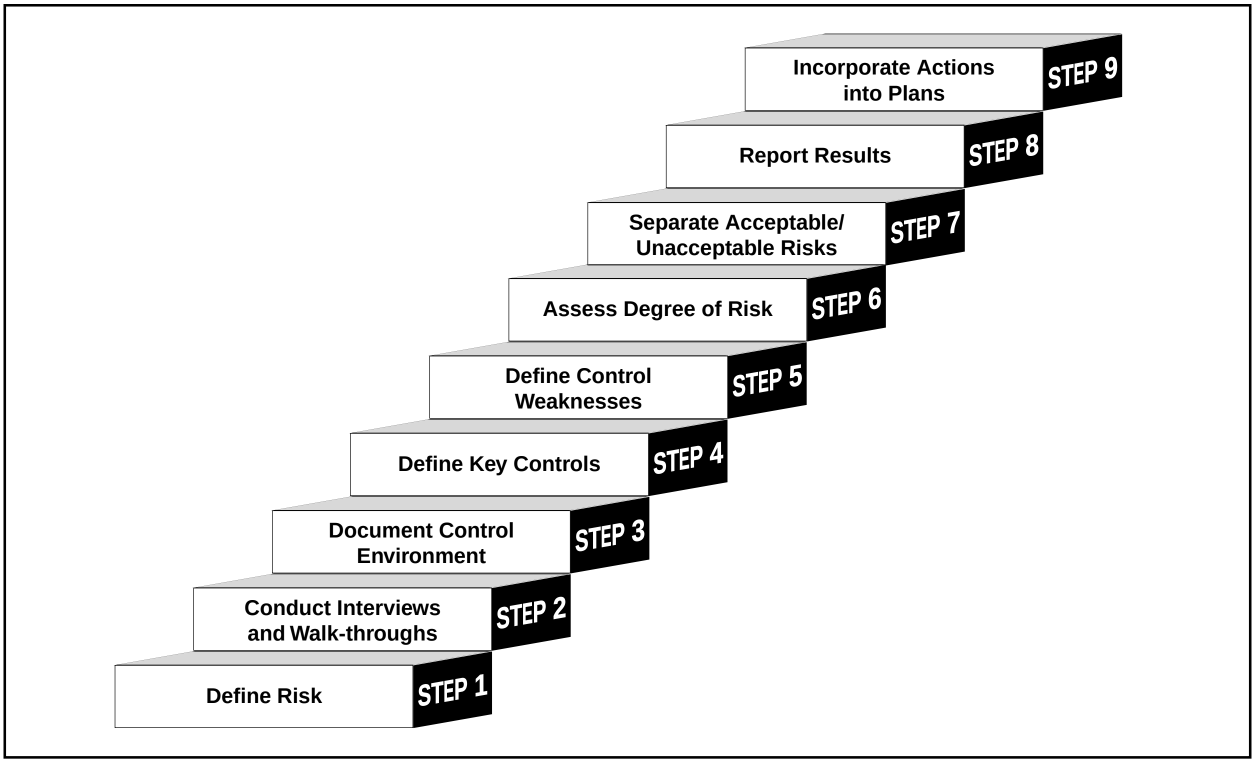
Incorporate Actions into Plans
STEP 9
Report Results
STEP 8
Separate Acceptable/ Unacceptable Risks
STEP 7
Assess Degree of Risk
STEP 6
Define Control Weaknesses
STEP 5
Define Key Controls
STEP 4
Document Control Environment
STEP 3
Conduct Interviews and Walk-throughs
STEP 2
Define Risk
STEP 1

Fig. 1. The risk-assessment process

in the control environment. They described what controls should be in place to safeguard assets but were not in place as well as what controls were in place but did not appear to be functioning properly. **(**Examples of control weaknesses are presented in Table 1**.**)

Step 6: Assess the Degree of Risk on a Control-by-Control Basis. The team summarized the control weaknesses by process (e.g., accessioning and cataloging), and by control type (i.e., inventory, physical, bibliographic, or preservation). For each weakness, the team assessed the degree of risk and whether management was willing to accept the risk. The degree of risk was measured by both the likelihood of occurrence and the magnitude of impact.

Step 7: Separate Acceptable Risks from Unacceptable Risks. All risks that management was willing to accept were removed from further consideration at this time. The risks that management was not willing to accept were sorted by level of risk (high, medium, or low) and by control type (bibliographic, inventory, preservation, or physical). Management analyzed the types of risks within each level to determine whether there were any pervasive weaknesses of a particular control type. This determination was based on several factors, including the probability that the weakness might significantly hamper the institution’s ability to carry out its mission.

Step 8: Report Results to Organization Management. The institution’s management team prepared an executive summary for organization management. The summary restated the institution’s mission and objectives, summarized the results of the risk assessment, and made conclusions about the effect of the results on the institution’s ability to carry out its mission and objectives. This report was used to support the institution's requests for further resources to strengthen controls or to institute additional controls that would facilitate achievement of the organization's mission objectives.

Step 9: Incorporate Action Plans into Management Performance Plans. After the risk-assessment results had been reported, management was expected to institute new controls or strengthen existing controls to reduce unacceptable risks. Management would hold itself responsible for accomplishing these actions by incorporating them into its annual performance plans or goals. It then would measure its own performance regularly to ensure the actions were taken and control effectiveness was improved.

Addressing Unacceptable Risks

The Library has now conducted risk assessments of most of its special collections, its general collections, and areas that perform essential activities to service the collections, such as the Preservation Directorate, the Copyright Office, and the Collections Management Division. It attempted to examine every type of collection item that carried specific risks so that it could extrapolate what had been learned to other similar materials that were not scheduled for assessment. This has allowed the Library to build a baseline assessment of risk and mitigating controls that meet the requirements of the audit process and yield critical information about the ongoing needs of the collections.

The final steps in the risk-assessment process are designed to summarize the results of the assessment and translate them into actions for management. Step 7 of the process separates acceptable from unacceptable risks. No situation or environment can ever be totally risk-free, and reducing risk costs money, whether in the form of additional insurance coverage or of funding to implement tighter controls. At this point in the risk assessment process, management must decide how much risk the institution is willing to accept—a decision that usually comes down to cost versus benefit, because no institution has unlimited resources. The impact of a high-risk behavior is obviously greater if the item at risk is a holograph Emily Dickinson poem rather than the second copy of the fourth edition of Joseph Heller's C*atch 22*. Similarly, risk may be unacceptable if a monograph is not cataloged or the number of copies the institution holds is not noted in a bibliographical database. In contrast, risk may be acceptable if individual pieces of a collection of manuscript correspondence do not receive item-level description, provided there are compensating controls in place.

For those risks that the institution decides it cannot tolerate, management must introduce mitigating control activities. Some risks can be overcome by changes in policies or procedures; overcoming others requires additional monetary or personnel resources. For instance, if the risk assessment reveals that existing physical security is inadequate, the institution will likely need to acquire security personnel or equipment to reduce the risk to an acceptable level. Securing funding for these improvements may remain a challenge, but with the risk assessment results in hand, managers will have the documentation necessary to support their requests as well as the business understanding necessary to present those needs to financial decision makers.

Monitoring Risk: An Ongoing Process

Assessing risk and identifying controls are just two steps in the business risk model. Controls are effective only if they are implemented, and they must be tested periodically to be sure they are operating effectively. Measuring process performance is one way to identify control failure, but constant monitoring is also essential. Monitoring involves assessing the design and operation of controls regularly and taking necessary actions. It applies to all activities in an organization.

For example, management may measure the performance of adequate preservation controls by recording statistics about how many items were treated during a particular period. However, this measure is meaningful only if management also had surveyed its materials and determined how many items were in need of treatment at the outset. This periodic evaluation is an effective monitoring tool to understand the general performance related to preservation, but it will not necessarily detect a specific item that needs attention.

Monitoring is also conducted by ongoing activities, such as noticing damage or deterioration of items that have been served to a researcher. If an item needs treatment, immediate action should be taken. Monitoring might also require thorough surveys of portions of a collection to see whether any items are particularly vulnerable.

Limitations on Internal Control

Management must be aware of what internal controls cannot do, as well as of what they can do. For example, internal controls, no matter how well designed, cannot provide absolute assurance that an organization's objectives will be achieved. All systems of internal control have inherent limitations. These limitations include faulty decision making, human errors, or collusion by two or more people within an organization. Management itself may also override controls. Therefore, while controls help ensure that management is aware of the organization's progress toward its objectives, they can provide only reasonable assurance that the objectives will be achieved. Above all, management should consider where controls, if instituted, will return benefits to the organization that outweigh their costs.

Long-Term Benefits of Risk Assessment

Integrating Technology

The future, many proclaim, is digital. Indeed, the present is largely digital as well. Library services have been deeply affected, and in some cases transformed, by the information technologies introduced since World War II. But while digital technology has transformed services by giving libraries spectacularly efficient, if not less expensive, ways of doing the traditional tasks of cataloging and maintaining inventory control, it is not clear how much the same technology will affect collections themselves. Are digital collections heritage assets? If so, what are the major risks to them and how should libraries safeguard them?

In most libraries, the internal control environments are deeply dependent on information technology (IT). The need for a robust technological infrastructure to support such things as online catalogs, circulation systems, creation of digital surrogates of collection items, and maintenance of copyright records means that IT managers bear a significant responsibility for the stewardship of heritage assets. In many libraries, the custodians of collections—librarians and curators—are culturally and physically far removed from the IT staff who are so critical to the well-being of the collections. Nonetheless, those who have direct custodial responsibilities for heritage assets and those who manage the controls over them are working toward the same objectives. To be effective in making collections accessible for the long term, IT managers and collections managers should cultivate relationships that support their complementary tasks. The risk-assessment process provides a framework for such partnerships.

A critical component of an internal control framework is the control environment, that is, the organizational culture. The control environment is improved when the organizational culture places a premium on the integrity and competencies of its people and makes each person’s responsibilities explicit and a factor in his or her overall performance evaluation. As an example, it may be convenient for staff working in a secured area to prop open doors at certain times of the day. It may also be convenient to send items to preservation for minor repairs without the custodial division filling out documentation to track the item. Nevertheless, these everyday behaviors are important components of a control environment. Another critical component is communication throughout the organization. One of the salubrious effects of a well-structured assessment of risk to collections is that each staff member who has some responsibility for protecting assets is identified and his or her role is made explicit. Because the process focuses on accountability at all levels of the organization, it can bridge the gap that often exists in large libraries between the content specialists (e.g., bibliographers, reference librarians, catalogers) and the infrastructure specialists (e.g., IT staff, security personnel).

There is no way to draw lines between the past and present of non-digital collections and the future digital library. Despite the connotation of the term “heritage assets,” these assets exist now in a hybrid environment of analog and digital services and controls, and the internal control framework of the future in which they will be managed will also be hybrid.

As libraries acquire more materials that are born digital, librarians will ask the same questions about how to manage and protect electronic information products as they do about their traditional resources. Digital resources come with many advantages. In theory, both inventory and bibliographical controls are easier to create and maintain (or they will be when common standards for description are defined). However, preservation and security risks loom much larger in the world of digital objects than in that of older materials. There is no way yet to ensure the longevity of digital data for a decade, let alone centuries. In addition, computer files, while hardly vulnerable to physical theft, reside on computer systems that may be vulnerable to viruses, invasion by hackers, and inadvertent programming disasters.

More problematic is the management of digital assets for long-term access. Because digital information does not reside on physical media or have its own independent physical existence, it is, in many ways, at much higher risk of loss or illegibility than are traditional resources. Digital information depends on hardware and software to decode the bits and bytes. It depends on metadata to identify its provenance and reliability. Most libraries have few policies and procedures that even begin to address, let alone ensure, the preservation of digital assets.

The business risk-assessment tool is well suited to the dynamic environment in which libraries now find themselves. In academic libraries, changing research trends alter the demand for and value of collection items. Materials deemed ephemeral and of low research value four decades ago are now heavily researched, and so the work of making those resources readily available has increased, as have the risks to those collections. Other collection items, once in great demand, now languish in storage areas, and libraries must provide optimal preservation conditions for their long slumber, waiting until new generations pose new questions and seek these old resources. The technology can also change demand for collection items. Special collections, for example, were long left in cataloging and processing backlogs. It was not worth the investment to process and preserve unique, but not often precious, special collections items, since they would always have a limited use by a limited number of people. It was thought better to catalog monographs and serials, which existed in multiple copies, had high use, and could be readily cataloged through shared databases. Digital dissemination has changed the way we value special collections. Nowadays, unpublished materials and visual resources are being preserved, cataloged, and scanned for digital access at many libraries and archives.

A similar changing demand in college and public libraries influences the controls that must be in place to ensure continued availability of their resources. Twenty years ago, public libraries did not have to worry much about videotapes and audio book tapes; however, that is far from the case today. How could a public library have anticipated and planned for meeting the growing demand for these resources? Annual reviews of the change in demand for and use of collection items, based on the baseline risk assessment that allows an institution to track trends, provide an excellent basis for identifying emerging needs and developing budgets. When something new appears in a library, be it a videotape or a computer file, it is initially acquired as an "add-on." Within five years or less, however, those new things become part of everyday business, and the funds to support them must come from within the library through budget reallocations. Every add-on in a budget inevitably results in a corresponding take-off. The regular assessment of heritage assets provides quick and quantifiable indicators of the change in value of a library's assets over time.

Taking Preventive Action

For libraries that are committed to retain collections long-term, materials that are no longer in demand are still assets that require protection. Preservation is the single most important investment that the library can make in its assets, and proper storage conditions can be the most effective preventive measure possible. The most vulnerable point in the life cycle of heritage assets is the moment when they arrive in the library. At that time, they have neither a bibliographical nor, perhaps, an accession record. After an item has received an identifying record, the greatest risk to fitness for use comes from the inherent instabilities of the physical recording medium and, when it is in use, from improper handling. Much work has been done in the past decade to determine the proper storage conditions for a variety of media. The removal of low-use paper-based items, film, and magnetic tape to off-site facilities built for preservation promises to be a boon to future generations of users.

Digital assets aside, preservation awareness and training are often the most cost-effective controls over heritage assets. Many preventive preservation measures do not require money, but rather staff training and small but important modifications in the behavior of both staff and patrons. Libraries are workplaces characterized by high levels of trust and professional pride. Requiring that staff check out books, even if they need them for only one day, or enforcing a similar policy for faculty members, may strike some as a subtle accusation. Nevertheless, the good stewardship of heritage assets is a responsibility of every member of the research community or general public that supports and uses a library. Library cultures are characterized by high levels of trust because American society places heritage assets in the public trust. Making members of the community aware of the risks to these assets and educating them about how they can help protect them does not lessen, but rather increases the chance that these assets will be accessible well into the future.

Appendix I: The Business Risk Model

The business risk model emphasizes meeting the goals and objectives of a mission-driven institution. For many research institutions, business risk is synonymous with the risk of failing to execute a program efficiently or effectively. A business risk model is suitable, therefore, for managing the cultural assets of nonprofit organizations. It offers a way to accord library collections their proper value as assets, not just costs; to assess the factors that might put the collections at risk of not serving their full function in mission work; and to determine how best to mitigate those risks in a cost-effective manner.

Determining Business Risk: Developing the Business Risk Model

It is important for an organization to identify the business risks that exist in the environment in which it operates. To identify those risks, organizations must review their external environments. External business risks stem from economic, political, social, environmental, technological, and other external conditions. For example, many research institutions face risks with respect to technology and customer demand. The electronic media in which research materials can be made available are creating a demand for faster search tools and for remote access to research materials. A library's ability to meet this demand and remain a well-respected institution is a business risk.

An organization cannot fully understand its business risks unless it also understands its business objectives, strategies, and processes. Figure 2 illustrates these interrelationships.

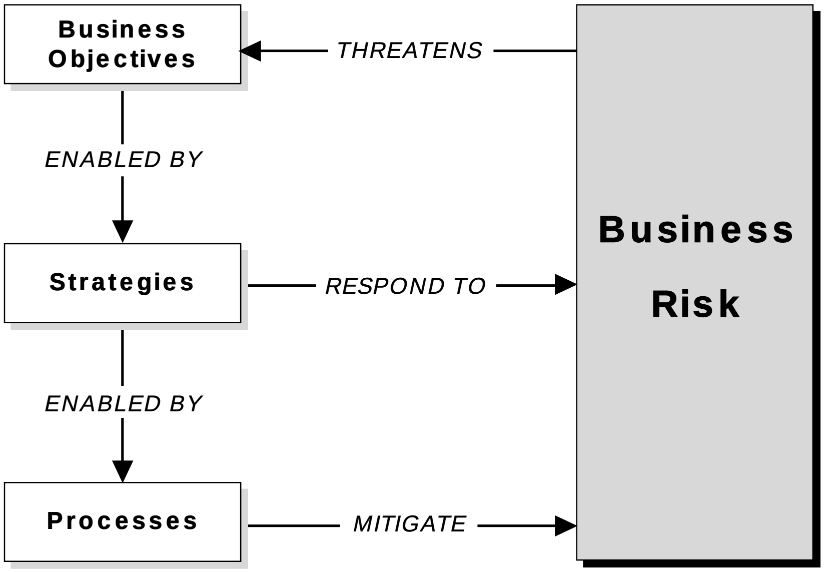

Fig. 2. Interrelationships between business objectives, strategies, processes, and business risk

As can be seen in the figure, the business objectives of an organization are continually threatened by risks. To respond to these risks, management develops strategies that enable the organization to meet its objectives. Strategies determine which business processes are necessary to meet management's objectives and which processes require controls to mitigate business risk.

No organization is immune to risk. Moreover, each organization's business risks change constantly. The nature and consequences of business risks facing organizations are becoming more complex and substantial. The speed of change, higher customer expectations, increased competition, rapid changes in technology, and countless other factors affect organizations in ways that managers are often unprepared to handle.

Risk is inherent in operating a business or running a program; an organization cannot eliminate business risks. Management has to decide how much risk is acceptable and to create a control structure to keep those risks within appropriate limits. The key to business risk management is achieving a proper balance of risk and control. An organization must expose itself to a certain level of risk to satisfy the expectations of its customers and stakeholders. A balance is achieved when the risk and reward expectations of stakeholders are understood and a system of controls that appropriately responds to the organization's risk exposure is in place. Therefore, a research institution's strategic management process should be designed to reduce business risk and attain its goals and objectives by implementing an appropriate and effective control environment.

If management fails to identify a significant risk or does not adequately consider business risks, the organization is unlikely to have in place control activities to manage those risks. Alternatively, if management does not consider environmental changes carefully, its existing control activities may no longer be adequate or appropriate. However, if an organization has a strong risk-management process, including an effective control environment, management can be reasonably sure that it has identified the significant business risks and responded to them appropriately. Figure 3 illustrates the typical flow of business risk-management activities.

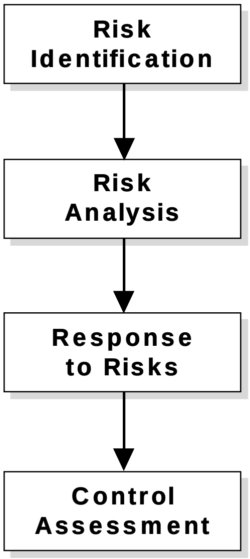

Fig. 3. Flow of business risk-management activities in an organization

The aim of risk management is to create an environment in which managers feel comfortable making decisions that entail risk. It is vital that risk management be linked to business strategies, so that decisions reflect both the desired risk tolerances of the organization and its strategic objectives. For instance, a library or research institution's mission may focus on providing timely and effective service to its researchers. To fulfill this mission, the organization must acquire the right kinds of materials and have them available when they are needed. If risks exist that threaten the organization's ability to acquire the right materials and make them available, controls must be established to minimize these risks.

Managing Business Risk

After identifying and analyzing business risks, management decides how these risks should be managed. This requires comparing the costs of reducing business risks against the costs of potential loss from risks. There are four categories of possible responses to business risks—accept, transfer, avoid, and reduce. The first three are passive responses to risk while the last response is active. The four categories may be defined as follows:

1. **Accept:** Accepting a business risk means doing nothing to avoid it. This response is based on a conscious decision that the costs of other responses outweigh the potential benefits or that the risk is acceptable.

2. **Transfer**: Transferring the business risk to another party alleviates management's responsibility for managing it. Examples of this response are buying insurance and outsourcing.

3. **Avoid**: Avoiding the business risk is a decision to change a business objective because no other response can reduce the business risks to an acceptable level in a cost-effective manner.

4. **Reduce**: Reducing the business risk means reducing either the likelihood of its occurrence or the magnitude of its impact. Management usually establishes an effective control environment to reduce business risks.

If management decides to actively reduce risk, it must develop an effective multilevel control environment. The control environment sets the tone of the organization. It provides (or fails to provide) the discipline and structural foundation for all components of control. The control environment also has a pervasive influence on how an organization sets objectives and structures its business activities.

A multilevel control environment consists of three elements: strategic, management, and process controls.

- *Strategic controls* refer to those activities within the strategic management process that help management to understand the effect of external and internal factors on the business and strategy. Strategic controls define the environment of risk and control behavior and align the organization with these strategies.

- *Management controls* are those activities and elements that must be present in the control system throughout the organization if it is to effectively identify, assess, and react to business risks and attain its objectives. These controls develop from the results of environmental review performed during the strategic planning process.

- *Process controls* are the control activities performed at the process, or function, level. They are normally the responsibilities of process, or functional, owners who ensure that the control activities are in place and meet their objectives. In the process of managing or serving collections, for example, the process owner would be a collection custodian, a librarian, or a library technician. The specific controls designed to safeguard research materials would be defined as process controls.

Strategic controls and management controls are implemented at the organization level, while process controls must be implemented for each business process. The acquisition, maintenance, and service of research collections are business processes. Management controls represent the link between the strategic level and process level, as well as among the processes themselves. Effective management control drives effective business risk and control management throughout the organization.

Most organizations do not establish a one-to-one relationship between business risks and mitigating controls. Therefore, it is important to understand the impact of a number of controls at different levels when assessing the strength of the control structure. Taken individually, single controls may not provide significant defense against a business risk. However, when reviewed as a whole, the interrelationship between differing types of controls can provide an effective armor of protection for the organization. Figure 4 shows the

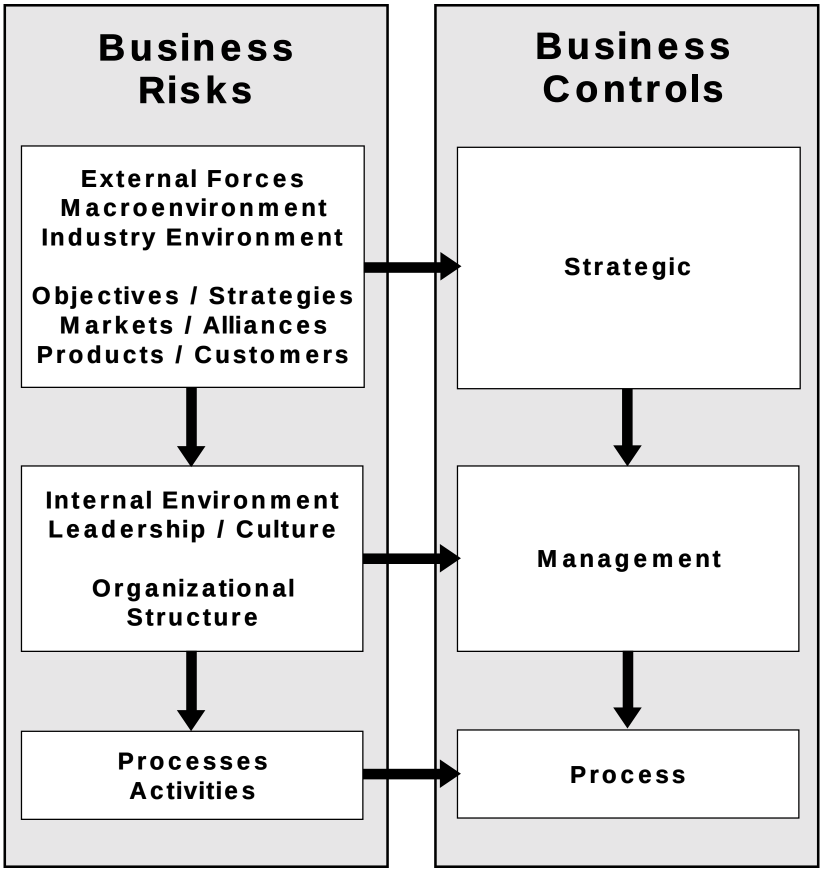

Fig. 4. Business risks and control elements at different levels of the organization

sources of business risks and the control elements at different levels of the organization.

There are two important control messages in strategic analysis:

1. Monitoring, assessing, and adapting to changes in the external environment are important aspects of managing business risk, particularly in the long term.

2. The tone set by management for the overall control environment and management's level of commitment to functional efficiency and effectiveness have a significant impact on an organization's ability to execute its strategies and achieve its business objectives.

Because external environmental factors and management's tone affect the organization's ability to meet its objectives, it is important that management understand the importance of these elements. In a research institution, for example, the increased demand for online research capabilities is an external environmental change. Management's ability to recognize that change and react responsibly to it, considering all risk factors involved in meeting that demand, is an example of strategic control.

Monitoring and Feedback

A good management system and control environment must have two important elements. First, the system should encourage clear and frequent communication of vision, strategies, and implementation in a way that allows all employees to recognize their roles and their importance in achieving business objectives. Second, the system should provide *relevant* and *balanced* feedback regarding performance against objectives. *Relevant* suggests clear connections to what is important for the business to achieve, and *balanced* refers to combinations of quantitative or qualitative, and financial or nonfinancial metrics to give management perspectives from both outside and inside the organization.

For example, if a research institution's mission is to provide timely and effective service to its researchers, a relevant goal is to make materials available within a certain time after they are requested. The feedback on performance of this objective is balanced if management measures a quantitative metric of "minutes researcher waited to receive requested materials" and a qualitative metric of "degree of satisfaction researcher expressed in service provided." These measurements assure management that they are focusing on both aspects of service, speed of performance, and quality of service.

Identifying Business Processes, Process Owners, and Measures of Performance

Organizations consciously identify the business processes that help them fulfill their objectives. Organizations divide their business processes into two categories: core business processes and internal service processes. Core business processes are those that an entity uses to develop, produce, sell, and distribute its products and services. Internal service processes provide appropriate resources to the other business processes. One of the core business processes of libraries and research institutions is the acquisition and management of research collection items.

A core process must have proper management controls to reduce those risks that threaten the institution's ability to meet its objectives. Two risks that threaten these objectives are not acquiring the right materials and not properly maintaining those materials. For each business process that is critical to the execution of business strategies, management controls should provide assurance that the best people are selected to own processes and control process risks. In a research institution, the process owners are usually researchers or librarians who hold management positions.

Management must establish clear objectives against which the process owners can measure their performance. Process owners are encouraged to assess their business risks continuously and to build cost-effective controls into the process to ensure that business risks are held to an acceptable level. Finally, process owners are held accountable for process performance, process risks, and the quality of the process controls. Therefore, monitoring business risks and controls is often an additional process-owner responsibility.

In Step 1, the process owner defines the process control objectives. An organization's control objectives can be related to its operations, its financial reporting, or its compliance with laws and regulations. The control objectives that are relevant in this report are the operation objectives. Operation objectives relate to achievement of the organization's mission—the fundamental reason for its existence. A clear set of operational objectives and strategies provides the focal point toward which the organization will commit substantial resources.

In Step 2, the process owner assesses business risk at the process level. After an organization has defined the objectives its process-level controls should achieve, the process owner must determine what controls are needed to achieve those objectives. This determination is based largely on anticipated business risk. Business risk is determined by understanding the internal and external factors that may affect the achievement of the process objectives. For example, if one of the objectives of a research institution's operational process is to negotiate acceptable prices for collection items, external factors such as inflation, supply and demand for the product, and competitors' actions may affect the degree of risk in achieving the objective. The mechanisms an institution builds into its procurement process to alert it to these events and enable it to respond favorably to them are examples of internal factors that affect business risk.

In determining the magnitude of business risk, management must estimate both the significance of the risk and the likelihood of its occurrence. For example, a potential risk that would not have a

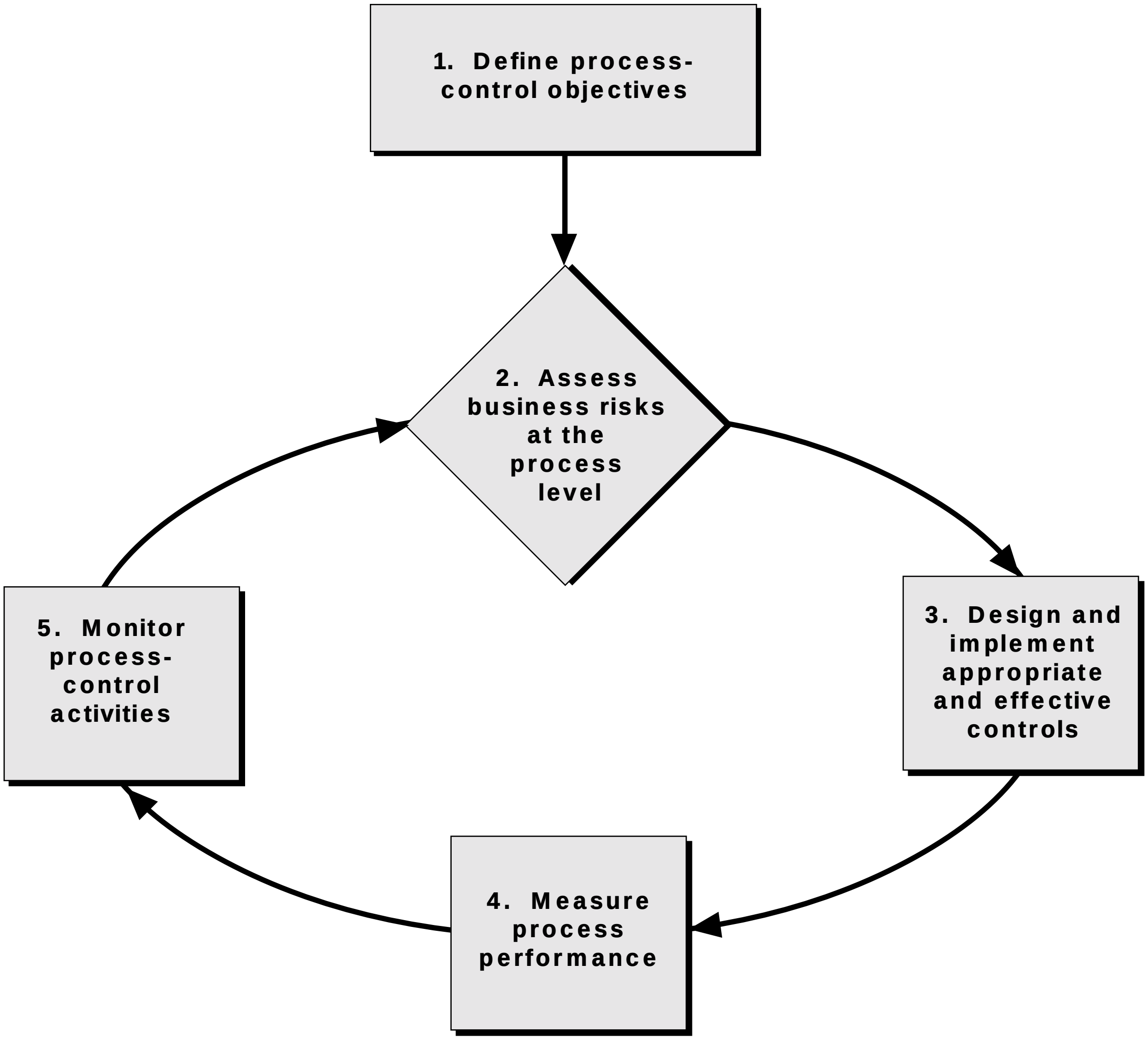
1. Define process-control objectives
2. Assess business risks at the process level
3. Design and implement appropriate and effective controls
4. Measure process performance
5. Monitor process-control activities

Fig. 5. Activities performed continuously by the process owner

significant effect on the operations of the process and that has a low likelihood of occurrence generally does not warrant considerable attention. Management should recognize that some degree of risk will always exist, because resources are always limited and all internal control systems possess inherent limitations.

In Step 3, the process owner designs and implements appropriate and effective controls for the process on the basis of the risk-assessment results in Step 2. Controls usually involve two elements: a policy to establish what should be done and procedures to carry out the policy. Controls serve as mechanisms for reducing business risk.

Because every organization has its own objectives and strategies, there will be differences in process controls among organizations. Even when organizations have similar objectives, process controls are likely to differ, because each organization has its own managerial style and culture. These differences influence the degree and type of business risks that similar institutions may face. The process owner should consider these differences when designing and implementing controls.

In Step 4, the process owner measures the performance of his or her processes. Each process owner should design quantifiable measures that can be used to assess whether the process is operating effectively. These measures, which are commonly referred to as *key performance indicators*, detect weaknesses in controls and changes in external conditions that are not reduced by process controls. The process owner should investigate unexpected results or unusual trends that may indicate that the organization's objectives are not being achieved. In the procurement process example, where the objective was to negotiate acceptable prices for collection acquisitions, the process owner might establish acceptable ranges of prices for certain types of collections on the basis of the average of prices for those items over a period of time. The process owner would be alerted to a possible control failure if the price of an item fell outside these ranges.

Step 5 requires the implementation of a process to monitor process control activities. This is an ongoing activity because internal control systems and the control environment change over time. New management may step in, information systems may be upgraded, or new personnel may need to be trained in the control policies and procedures. Monitoring ensures that internal control continues to operate effectively through all these changes.

Examples of ongoing monitoring activities include the following:

- Communications from external parties either corroborate internally generated information or indicate problems. For example, customers implicitly corroborate billing data by paying their invoices. Customer complaints, by contrast, may signal billing system deficiencies.

- Supervisory activities provide oversight of control functions and identification of deficiencies. For example, review activities serving as a control over the accuracy and completeness of cataloging record entries are routinely supervised. Alternatively, duties of individuals are segregated so that employees serve as checks on each other. This deters fraud because it inhibits the ability of a staff member to conceal suspect activities.

- Data recorded by information systems are compared with physical assets. Inventories of research materials are examined and counted periodically. The counts are compared with accounting records, and differences are investigated.

- Operations personnel are requested to state whether certain control procedures, such as reconciling specified physical amounts to recorded amounts of items in their process, are regularly performed. Management or internal audit personnel may verify such statements.

The Library Manager as Process Owner

In a library or research institution, the five process-owner activities just described might be performed in the following manner:

Step 1. Define process-control objectives. The institution's mid-level management receives the organizational objectives from upper management. The organizational objectives include an objective related to the mission of the library or research institution such as "to serve the research community by consistently providing timely and effective service." The management of the library identifies those processes that directly address this mission and further identifies the objective of those processes. For instance, acquiring and replacing research collection items is a process designed to maintain the collection so that it is an effective research tool.

Step 2. Assess business risks at the process level. The library manager determines what business risks might prevent the institution from providing timely and effective service. Each risk is then ranked based on the likelihood of its occurrence and the expected magnitude of impact, should the risk occur. For instance, the institution may lack the technology necessary to provide quick searches for research materials by subject. The library manager assesses the likelihood that timely and effective service will not be provided, as well as how many researchers this might affect and to what extent. The manager makes a judgment about the degree of this risk and determines what controls should be instituted to mitigate it.

Step 3. Design and implement appropriate and effective controls. The library manager identifies what controls are necessary to reduce the risks of not meeting the process objectives. For example, to provide timely service, the institution may have instituted a priority service for its most frequent customers or its most recognized scholars. Alternatively, it may have measured and quantified its service requests over a period of time and developed librarian and technician schedules based upon when demand is expected to peak and recede.

Steps 4 and 5. Measure process performance and monitor process control objectives. The library manager should measure process performance and monitor process control activities. He or she can measure performance in providing timely and effective service by using customer satisfaction surveys and by periodically measuring the volume of customers served. These measurements should be reviewed and tracked to determine whether performance is improving or deteriorating. This monitoring function alerts management that controls are either not operating properly or are ineffective; on the basis of this information, management can determine what action needs to be taken.

The management controls that reduce the business risks associated with serving researchers include controls to safeguard research materials. These controls can take various forms, depending upon their purpose and the type of assets they are controlling. By looking at these safeguarding controls from a business perspective and linking them to the organization’s mission, managers gain the insight necessary to protect and preserve their collections.

Step 2 of the process just described, (i.e., “Assess business risks at the process level”) was the basis for the collection risk assessments that were performed by the Library of Congress, with assistance from KPMG LLP, from 1997 through 1999. The risk-assessment process conducted by the Library is described in the main body of this report.

References

Caltech. 2000. Mission Statement. Available from http://library.caltech.edu/about/mission.htm.

Committee of Sponsoring Organizations of the Treadway Commission (COSO). 1991. *Internal Control—Integrated Framework.* New York: Committee of Sponsoring Organizations of the Treadway Commission.

Denver Public Library. 2000. Mission Statement. Available from http://dpl20.denver.lib.co.us/dpl/aboutdpl.html.

Library of Congress. 1997. *The Library of Congress, Financial Statements for Fiscal 1996*, p. 1-1. Washington, D.C.: Library of Congress.