CHAPTER II: INTERNAL CONTROLS

CHAPTER CONTENTS

Section A. Introduction

What type of bookkeeping system should be used? How many bank accounts are needed? Who should be able to sign checks? Who should deposit the weekly receipts in the bank, and how? These are just some of the questions to be answered when setting up an accounting system for a congregation. Such questions should be periodically reviewed.

Often, many of these decisions are made without adequate thought. Others may require more deliberate consideration. Altogether, the decisions that are made become the policies and procedures of the accounting system and are referred to as "internal controls." Good internal controls will ease the treasurer's job. They the guidelines that provide greater assurance that transactions are recorded properly, that the records are reliable, and that church assets are protected. They also assure compliance with civil laws, church canons, and organizational policies.

A system of internal controls consists of all measures used by an organization to safeguard its resources and ensure accuracy, efficiency and reliability in accounting and operating information.

It is important to emphasize that internal controls are designed to prevent or identify inadvertent errors as much as they are intended to prevent the deliberate theft or misuse of funds. Without an appropriate system it is not possible to assure the reliability and integrity of the records or reports generated by an organization.

An effective control system ensures that procedures exist that meet the following objectives:

1. Adequately safeguard the cash, property and other assets of the office.
2. Ensure that all financial transactions are appropriately documented and approved by authorized staff.
3. Ensure that funds are expended in accordance with donor requirements and limits.
4. Ensure that financial reporting is accurate, timely and conforms to policies.

The overriding objective of all controls is to reduce cost-effectively the risk of loss or misuse of funds or property to a tolerable level. Obviously, not all the controls will apply to or be cost-

effective for all types of operations. Appropriate consultation is encouraged whenever there is a feeling that certain controls may not be cost-effective for their operations.

Section B. Internal Control Concepts & Considerations

Conflict of Interest

In all matters related to the parish, all employees, clergy and vestry are expected to avoid conflicts of interest and have a duty to disclose all instances of apparent or potential conflicts of interest. A sample Conflict of Interest Policy is found in the appendix to this chapter.

Segregation of Duties

Essential to the control system is the concept of segregation of duties. Every financial transaction involves five steps.

1.	Request	request to purchase
2.	Approval	authorized personnel approve request
3.	Authorization	approval to purchase, issuance of purchase order
4.	Execution	purchasing, receiving and payment
5.	Recording	accounting

No one person should handle all aspects of a single financial transaction. For each transaction the responsibility for authorization, accounting for and custody of the related assets must be separate.

1) The custody of assets must be separate from the responsibility for accounting for these assets.

2) The authorization of transactions must be separated from the custody of related assets. For example;
   a.) The warehouse staff distributing goods should not be able to approve the distribution of goods.
   b.) Cashiers cannot be authorized to approve cash disbursements.
   c.) Program staff approving the purchase of supplies may not also keep the program supplies inventory.

3) The authorization of transactions must be separated from the accounting for the transactions. For example:
   a.) Check signers should not also be authorized to approve accounting transactions.
   b.) Staff authorized to hire employees or temporary labor should not be able to approve the payroll accounting entries.

4) For procurement activities attention must be paid to separating the authority for the selection of vendors, bidding process and approval of the final supplier. For example:
   a.) The person responsible for maintaining the vendor list should not authorize the final selection of a supplier.
   b.) The person soliciting bids cannot be responsible for maintaining the vendor list.

Authority Levels
Control systems can only function effectively when all employees know who within the organization has the responsibility and authority to initiate or approve expenditures or the use of other assets. These responsibilities and authority levels must be specifically defined and structured to reflect the knowledge and responsibility levels of the various positions within the organizational structure.

Employees assigned the authority to approve and/or authorize commitments or expenditures must:
1. Be given written notification of their authority levels and limits. (This may be included in their job description)
2. Be fully conversant with the required procedures and documentation before approval can be given to commitments or expenditures.

Authorization List(s)
1. e

Payments & Cash Disbursements
In addition to authority levels for commitments, each organization needs to assign authority levels for payments/cash disbursements. It must be emphasized that approving the payment of a commitment involves ensuring that either the required goods or service have been received and that all supporting documentation has been presented.

Accounting Transactions
The finance staff should not be able to authorize the transactions they are responsible for recording. This is a basic requirement under segregation of duties.

Documentation & Record Keeping Standards
Financial activities and transactions must be clearly and appropriately documented, recorded and maintained according to the minimum recordkeeping policy (see Records Management for Congregations published by the Archives of The Episcopal Church at https://www.episcopalarchives.org/sites/default/files/RecManManual_rev_07-2017.pdf).

Documents must be safely stored to prevent loss or damage. An appropriate filing system and/or storage system for historical records needs to be in place to ensure that documents can be located when required.

To maintain uniform standards of documentation and record keeping, systematic procedures need to be in place that incorporate standard forms, approval processes and accounting procedures. An up-to-date policy and procedures manual, which clearly specifies these procedures, is essential in maintaining adequate documentation and record keeping.

Independent Reviews
The control features discussed are all used in day-to-day processing of activities and accounting. However, regardless of how good a system is, errors will be made, and circumstances will change that will require changes in the control system.

Procedures need to be in place to ensure periodic independent reviews are performed. For example:

- Someone not involved with cash or accounting should perform periodic surprise cash counts.
- Program staff and management should review monthly expenditure reports.
- Inventory, or supplies, should be independently counted and verified to the bin cards/logistics system & accounting records.
- Annual performance evaluations should be required for all staff, utilizing a standard format and review process.

On an annual basis, a formal review should be implemented of the controls in place, authority levels and procedure manuals.

Cash

Cash is the most liquid of assets and is most likely to be misappropriated. For this reason, establishing basic internal controls over cash receipts, maintenance of cash and cash disbursement is critical.

Risks with cash are:

1. Theft or loss of cash.
2. Disbursement of cash without proper documentation or authorization.
3. Incorrect charging of receipts/disbursements (i.e., to incorrect source codes or accounts).

Reconciliations & Verification

Standard reconciliations and independent verification are essential to maintaining the integrity of control over cash.

Physical Cash (petty cash and cash-in-office)

1. Petty cash balances should not exceed $1,500.
2. The petty cash log should always be complete (e.g., petty cash on hand, plus receipts should equal the original petty cash balance).
3. Petty cash should not be used as an operating fund (not used to pay for goods or services, salaries, etc.).
4. Petty cash funds should be maintained in a secure area such as a locked drawer or small safe.
5. Custodian should replenish funds when the cash balance is low, as well as periodically close inactive accounts.

Payroll

The major risks associated with payroll are:

1. Failure to appropriately terminate employees
2. Failure to adhere to laws and regulations
3. Overpayment to legitimate employees
4. Payment of fictitious persons
5. Failure to recover advances
6. Misappropriation of payroll funds

7. Under or overpaying withholding taxes

Required Forms

In order to avoid confusion or misunderstanding among staff members about salaries and benefits, all payroll related activities must be clearly and consistently documented. This documentation is key to good internal control over the payroll process.

The following types of forms are recommended:

1. Employee Employment Letter
2. Employee Timesheets – for recording hours worked, by grant, and absences
3. Employee Leave Form – for requesting and approving leave time
4. Employee Action/Change Form – for recording changes in salary, title, benefits or other pay related actions
5. Employee Termination Form – for recording the termination of a person from the payroll
6. Salary Advance Form – for requesting salary advances, repayment date should be specified (i.e. next payroll date)

Personnel

Competent, trustworthy personnel are essential for an effective internal control system. Hiring or retaining dishonest or incompetent staff is a major cause of the loss or misuse of assets.

1. Staff must be hired on an unbiased basis, and candidates selected on qualifications and experience to avoid or minimize conflicts of interest.
2. A standard performance evaluation process will recognize good performance but must also identify underperforming staff so that appropriate corrective action can be taken either to improve performance or remove the employee.
3. Employees can only fulfill the requirements of their position if the requirements are clearly communicated. Every employee must have an up-to-date job description, which clearly states his/her duties and responsibilities.

Procurement

Management of procurement should be a top priority.

The major risks associated with procurement are:

1. The wrong items are purchased;
2. The correct items are purchased but at a price that is higher than necessary (either through error or through improper dealings with vendors);
3. Items of inferior quality are purchased;
4. Purchases are made without sufficient budgeted funds;
5. Purchases are not in compliance with donor regulations or terms of grant agreements;
6. Purchases did not go through appropriate sourcing channels.

Suggested Forms

All organizations should consider using the following types of forms for purchases. (The list may be shortened for very small organizations.)

1. Purchase Requisition
2. Standard Bid Request
3. Bid Summary Worksheet
4. Purchase Order
5. Receiving Report

Vendor List

Ensuring the use of reliable vendors , competent to deliver and independent of any relation to the organization or its staff, is essential to a good procurement system. Using a standard vendor list aids in ensuring transparency in the procurement process and minimizes conflict of interest situations.

(1) An acceptable vendor list should be developed and maintained.
   a) This list should include the name of the vendor and what types of goods or services it provides.
   b) Those developing the list should include reliable vendors, whose recommendation has come from an outside organization , from published material and from employees who are familiar with the vendor.
   c) At least three vendors for each type of good or service purchased should be included in the list. When fewer than three reliable vendors are identified, the staff should confirm and document in writing that fewer than three reliable vendors exist for a given type of procurement.
   d) The vendor list should be revised periodically (at least annually), based on formal feedback that the procurement department obtains from other employees on the quality of procurement from a given vendor. The feedback should be reviewed to determine whether it has been considered in revising the list.

(2) Access to making changes to the vendor list should be restricted to those employees assigned the responsibility of developing and maintaining the list.

(3) Those employees who solicit bids should not be involved in developing or maintaining the vendor list or have access to making changes in it.

(4) The employee assigned to establish and maintain the approved vendor list should not be the same employee who solicits bids or who selects the wining bidder.

Purchasing Process

1. A purchase requisitions form, signed by the requisitioner and approved by his/her supervisor, or next higher-level employee with sufficient authority to approve, must be prepared for all procurement.
2. The employee approving the requisition must ascertain that sufficient funds remain in the budget to make the procurement and that the procurement is necessary to achieve objectives.
3. The employee initiating the purchase request should not approve the request.
4. Before executing a procurement transaction, procurement personnel must determine whether those signing the requisition form have authority according to the established Authorization List.
5. Procurement personnel must solicit at least three written, independent bids for procurement above a certain dollar amount. Bid solicitations should include a detailed description of the items, specifications, maximum cost, and quantity along with a required delivery date.

6. The person soliciting the bids should not approve the vendor selection.
7. Sealed bids should be required for procurement above a certain reasonable limit (e.g., $250,001 as outlined in the Uniform Guidance established by the US Office of Management and Budget). Vendor selection should be unbiased.
8. A bid summary worksheet should be completed for all procurement requiring bids. The worksheet should document the reason for selecting the vendor and should be signed by an authorized employee as evidence of review and approval.
9. Requisitioners should be discouraged from making purchases themselves. The procurement unit should purchase as many items as possible and all items costing more than $500.
10. Centralized purchasing and blanket purchase orders of office supplies, spare parts, etc. are encouraged in order to take advantage of vendors' quantity discounts .

Procurement Personnel

Procurement personnel and any other personnel involved in the vendor selection process are prohibited from accepting anything of value from vendors or potential vendors.

Personnel should be required to sign "conflict of interest" statements clarifying that neither they nor their immediate family members have any equity in any of the vendors awarded purchase contracts nor would stand to benefit personally from awarding contracts to a given vendor.

Commitment tracking

- Most financial systems do not track commitments. An alternative system should be implemented to track outstanding purchase orders and subcontracts.
- As part of the approval of new purchases, outstanding commitments must be considered in order to avoid overspending the budget.

Cash Advances

The risks associated with cash advances are that they are not liquidated in a timely manner and that their liquidation is not based on proper documentation.

Advances are funds provided to employees to pay for business expenses. The two types of advances are project advances and employee advances. Project advances are provided for project expenses, typically when cash is not readily available from the source where disbursements are usually made. The person receiving the advance liquidates it by providing receipts totaling the amount of the advance and/or by repaying it in the original currency advanced. Employee advances typically cover travel expenses. In this case, the employee liquidates the advance by submitting a Travel Expense Report with supporting documentation.

Procedures to ensure adequate control would include:

1. A written approval process for employee advances (i.e., who has the authority to approve the advance).
2. A policy should be established that precludes an employee from obtaining an advance if he/she has an outstanding advance, or that places a limit on the number of outstanding advances allowed an employee.
3. A monthly review of advances is recommended in order to identify any advances outstanding for more than 30 days. Advances outstanding for more than a year should be withheld from the employee's salary.

Information Technology and Telecommunications

A parish (mission, diocese, etc.) should commit to having its "Information Technology and/or Telecommunications Systems" (including, but not limited to, computers, networks, Internet access, Intranet access, e-mail accounts, telephones, voice mail, organization-issued or owned cellular phones, smart phones or similar devices and/or any other means of communication known or hereafter developed, and provided cellular phone service, PDA smart phones or similar device service and/or any other communication service known or hereafter developed) used in a responsible, efficient, ethical, and legal manner, and to safeguarding its information assets. Parishes should also make certain, to the extent possible, that all confidential information is kept confidential.

The Parish should adopt a policy that provides:

1. All data on the parish's Information and/or Telecommunication Systems, unless otherwise available in the public domain, are classified as confidential and/or proprietary.
2. Unauthorized use, destruction and/or modification of the Parish's Information and/or Telecommunications Systems are strictly prohibited.
3. Parish information and/or Telecommunications Systems are provided to employees for official parish business. Employees may use these resources for incidental personal use, provided such use does not interfere with employee productivity and/or parish operations and is consistent with parish policies and all applicable laws.

4. Employees do not have an expectation of privacy in anything they create, store, access, send, or receive on the parish Information and/or Telecommunications Systems. The parish has the right, but not the duty, to monitor any and all of the aspects of its Information and/or Telecommunications Systems.
5. The parish reserves the right to use software to identify any Internet site(s) that it deems inappropriate, illegal, sexually explicit, or violates applicable equal employment opportunity principles and any policies against harassment and other discrimination.
6. Any attempt to circumvent parish security procedures is prohibited.
7. Employees must ensure that personal blogging and social networking activities do not interfere with work assignments or disseminate information in a manner bringing disrepute, damage, or ill-will against the parish.
8. Employees cannot use parish-owned facilities or equipment, including computers, licensed software, or other electronic equipment, to conduct personal blogging activities. Employees are reminded that they should have no expectation of privacy.
9. Users of parish Information and/or Telecommunications Systems must comply with all laws regarding the use of such devices while driving. Electronic devices should be used only when it is safe to do so under the circumstances and users must be aware that, even with a hands-free device, electronic devices should not be used during adverse weather or difficult traffic conditions.
10. Cellular phones/smart phones purchased by the parish and issued to employees are the property of the parish.
11. Individuals assigned cellular phones/smart phones are responsible for safeguarding them from damage and misuse.
12. The parish reserves absolute discretion and control over whether, and if upon what terms (*e.g.,* minute allotment, personal use, cost to employees, etc.), to issue cellular phones/smart phones or other electronic devices and/or to provide cellular phones or other electronic services to employees.

Section C. Electronic Banking

Electronic banking provides a faster, easier, and efficient substitute for paper processing and recording receipts and disbursements. Electronic banking uses computer and electronic technology to streamline process, while reducing the cost of transactions. Banking can be done without leaving the office, generally at any time of the day and, often, it is possible to can see up-to-the-minute balances and recorded transactions. Receipts, disbursements and transfers in most circumstances can be processed via electronic funds transfer (EFT) services, whether transferring funds from a savings to a checking account at the same bank or making a payment to a vendor's bank across the country. **Traditional internal controls, such as written policies and procedures, authorizations, segregation of duties and monitoring are important when using electronic banking.**

Policies and Procedures

Before electronic processing is begun, detailed policies and procedures should be in place that specify the online banking activities and electronic funds transactions in which the organization engages. The policies should include the following:

- What online banking and EFT activities will be used
- Who has the authority to establish an electronic bank account
- Who is authorized to initiate electronic transactions
- Who will approve electronic transactions
- Who will transmit electronic transactions
- Who will record electronic transactions
- Who will review and reconcile electronic transactions?

This policy must be consistent with the statutory and other legal responsibilities of the officers and employees involved. It is advisable to have all employees who engage in electronic banking activities to participate in training that helps them identify various technology threats.

Segregation of Duties

Classic internal controls, if well designed, work well with EFT technologies. Proper segregation of duties is important in almost any business function but is critical for electronic transactions. Without proper segregation of duties, the risk increases that one person could be in a position both to commit a wrongdoing and to conceal it. At least two individuals should be involved in each electronic transaction. The authorization and transmitting functions should be segregated and, if possible, the recording function should also be delegated to someone who has neither approval nor transmitting duties. Generally, the same controls should be used for electronic disbursements through online banking as apply to the manual preparation of checks. Payments made using electronic funds transfer services cannot circumvent laws, regulations, and/or the internal control policies.

Electronic or Wire Transfers

Electronic or wire transfers are transfers of funds that are usually effective within minutes of being executed. For wire transfers, a secure ID Access should be required (e.g., an RSA SecurID authentication mechanism).

Safeguards

Some banks offer electronic or wire transfer capability in their online banking programs, allowing input of the required information to initiate, authorize and transmit wire transfers in-house without outside assistance from a depository. Access to in-house electronic or wire transfer software should be controlled, and its use should be authorized and monitored frequently due to the ease with which transfers can be

made. Safeguards for initiating an electronic or wire transfer include phoning the bank and using a password to authorize the transfer verbally, hand delivering a letter of authorization to the bank with the transfer instructions or sending a fax with the authorized signature and password.

Before an organization opts to disburse funds by electronic or wire transfer, the governing board is required to enter into a written agreement with the bank or trust company in which the funds have been deposited, including implementation of a security procedure. There should be a callback provision in the electronic or wire instructions that requires the bank to call a staff member other than the person initiating the transaction to confirm the appropriateness of the transfer. Additional controls can be established as well (e.g., a policy that does not allow the bank to initiate wire transfers out of the country).

Monitoring
An internal control system must include procedures or safeguards for the documentation and reporting of all fund transfers and disbursements by electronic means or wire. In addition, the bank or trust company must provide the officer requesting the transfer with written confirmation of the transaction no later than the business day after the day on which the funds were transmitted.

Electronic Check Images
Most banks no longer provide cancelled paper checks to their customers but offer electronic check images online or on CD. These electronic images may be accepted in lieu of cancelled checks, upon authorization by the governing board.

Provider Responsibilities
Although customer protection and privacy regulations vary between jurisdictions, banks generally have a clear responsibility to provide their customers a level of comfort regarding information disclosures, protection of customer data and business availability that approximates a level used in traditional banking distribution channels. To minimize legal and reputational risk associated with e-banking activities, banks should make adequate disclosure of information on their web sites and take appropriate measures to ensure adherence to customer privacy requirements applicable in the jurisdictions to which the bank is providing e-banking services.

E-banking services must be delivered on a consistent and timely basis in accordance with customer expectations for constant and rapid availability and potentially high transaction demand. A bank must have the ability to deliver e-banking services to all users and be able to maintain such availability in all circumstances. Effective incident response mechanisms are critical to minimize operational, legal and reputational risks that may arise from unexpected events, including internal and external attacks, that may affect the provision of e-banking systems and services. The bank should also have effective capacity, business continuity and contingency plans, including communication strategies, that reassure its customers.