Orientation to Internal Controls

Internal controls are a cornerstone of strong financial management in Employment Social Enterprises (ESEs), helping safeguard resources, build funder confidence, and ensure mission-aligned use of funds. This guide introduces the concept of internal controls, outlines different types, and provides practical examples to help ESEs assess their needs. This guide will:

- Clarify what internal controls are and why they are essential to ESE financial health and accountability.
- Help ESE leaders reflect on which controls are most relevant to their organization.
- Explain the three categories of internal controls—preventive, detective, and corrective—with practical examples.

CONTENTS

Introduction

Internal controls are practices and procedures that are put in place at an organization to prevent, detect, and correct error and fraud. Internal controls are essential for employment social enterprises (ESEs) because they:

- **Reinforce the financial health of the ESE** by ensuring that cash and other assets are being managed well and directed towards the mission
- **Give confidence to donors, investors, and partners** that funds are being used in the manner for which they were intended, thus encouraging ongoing or increased funding
- **Ensure that organizational assets are not being used for illegal or unapproved purposes** which could put the ESE at legal risk, potentially undermining its impact and ability to operate
- **Help with regulatory compliance** such as financial reporting to government entities
- **Support ongoing operational efficiency** by establishing and continuously improving processes that reinforce transparency and cross-organizational communication

Risk Assessment: Determining Where Your ESE May Need Internal Controls

Before implementing any internal controls, ESEs should conduct a risk assessment to identify areas most susceptible to fraud, errors, or inefficiencies. This helps prioritize the controls that will be most effective in safeguarding financial assets.

A risk assessment doesn't have to be overly complex or time-consuming. In fact, for smaller ESEs this can be done within a day or week. ESE leaders and key stakeholders (such as board members) can complete this by determining where the greatest financial risks lie when it comes to the ESE's financials (as any given ESE will be unique in where it has the greatest risk exposure). As an example, an ESE that has a lot of cash-based transactions (e.g., landscaping customers paying for their services in cash) will require a different set of controls from another ESE that doesn't.

When conducting a risk assessment for your ESE, consider:

- **Whether your ESE has high-risk financial transactions** – These could be transactions that are either large amounts, very frequent, or subject to limited oversight due to the nature of the transactions (e.g., cash payments from landscaping customers). Consider which kinds of transactions are the highest risk for your ESE, and which controls will help to reduce the risks.
- **Whether there are unique external threats –** Depending on a number of factors, your ESE may face risks outside of your ESE. Do a majority of your transactions occur digitally, and/or require storing your customers' financial data? Then there may be a high risk of cyber fraud for your ESE – external entities may try to exploit vulnerabilities in your systems in order to benefit from stealing data or accessing accounts.
- **Whether there are internal vulnerabilities –** It's important to reflect on how well your ESE is protecting itself from internal risks and what can be done to address those vulnerabilities. Does only one person manage the entire payroll process? Are keys to the office given to only designated personnel, and collected if those individuals leave the ESE for any reason?

Types and Examples of Internal Controls

Internal controls fall into three broad categories – Preventive, Detective, and Corrective. Remember that an internal control is intended to prevent risk or to address potential negative impact of a risk to your ESE. Any given risk identified during your ESE's risk assessment can be prevented or addressed by one or more internal control and each internal control will fall into one of these categories. Below you'll find a definition of each of these categories, along with examples of how these internal controls *might* look in your ESE. Keep in mind that these are only examples and are neither prescriptive *nor* exhaustive – as you read through these examples it's important that you evaluate whether this is a scenario that is relevant to your ESE and if the illustrated internal control could be applicable to your organization before taking action to implement controls.

Preventive Controls: Preventing errors or fraud before they occur

Preventive controls are designed to **reduce risk before** any fraud or errors take place. Preventive controls are policies and processes that include restricting access to financial management systems, establishing approval processes, and segregating duties.

Table: Preventive Controls

Preventive Control	Description of this control	What a real-life "risk scenario" might look like that this control is intended to *prevent*	What it could look like to implement this control to address this specific real-life "risk scenario"
Segregation of duties	Ensures that there is not one single person with control over a particular financial process or transaction.	An employee with the ability to both enter and approve payroll data increases their salary without oversight or authorization.	Ensure one person enters payroll data (hours worked, wages, etc.) and another approves payments before processing.
Establishing authorization & approval policies and processes	Requires approvals for certain types or amounts of expenditures.	A staff member signs a $10,000 vendor contract for training services without leadership approval. The training later turns out to be unrelated to the workforce's needs and can't be refunded.	Establish thresholds for expenditures, requiring specific approvals for those within certain ranges: Below $1,000: Program Manager $1,001 to $5,000: CFO or Director of Finance Over $5,000: ED/CEO and Board Chair [1]
Setting spending limits on debit/credit cards	Restricts how much and what type of purchases can be made using organizational credit or debit cards, helping prevent unauthorized, accidental, or fraudulent expenditures.	A case manager uses a debit card to purchase $1,200 worth of grocery gift cards for participants. Unfortunately, the entire amount exceeds the allowable benefit cap per participant and violates a funder's restriction, thus putting the program's funding at risk.	Issue program-specific cards with a $500 per-transaction cap and a $1,000 monthly spending limit. Use expense management tools to automatically alert the finance team when certain limits are reached.[2]
Establishing access controls	Controls that limit who can access sensitive physical and digital financial assets, systems, and records, ensuring that any access is granted only to those who need it.	A former employee still has login access to the accounting system after termination. They use their credentials to download confidential payroll data, creating a serious data breach and exposing the ESE to legal liability for stolen personal information.	Require unique user logins for all financial systems. As part of HR's termination checklist, include a step that ensures terminated employees' access is removed within 24 hours.

[1] These thresholds can vary from organization to organization.
[2] Expense management tools can help to automate controls in this category. See the "Resourcing Financial Management in ESEs Across Stages of Growth" guide for more information on systems that may be relevant to this situation.

Detective Controls: Identify errors or irregularities when they occur

Detective controls are procedures and practices designed to identify errors, irregularities, or fraud after they have occurred. They help uncover issues through activities such as regular monitoring, reviews, and audits so that corrective action can be taken promptly.

Table: Detective Controls

Detective Control	Description of this control	What a real-life "risk scenario" might look like that this control is intended to *detect*	What it could look like to implement this control to address this specific real-life "risk scenario"
Performing regular reconciliation of accounts	The process of comparing internal financial records (e.g., from accounting software or spreadsheets) with external records (e.g., bank statements) to detect discrepancies like missing transactions, duplicate payments, or fraud.	A staff member mistakenly enters a $950 payment to a vendor twice in the accounting system. This duplicate payment isn't caught until months later when the vendor has already cashed both checks and the ESE can't recover the funds.	Schedule regular monthly reconciliations for all bank accounts, led by someone not involved in issuing payments. If using accounting software, use the reconciliation feature to facilitate the process.[3]
Regularly reviewing budget to actuals	A routine comparison of budgeted revenue and expenses to actual financial results, helping organizations detect overspending, underperformance, or unexpected trends.	An ESE projected $25,000 in earned income from their café for the first 3 months of the fiscal year. But after six months, only $9,000 has come in. Since this was a critical source of cash for the ESE, this shortfall forced unexpected program cuts.	Establish quarterly budget-to-actuals reports for each program and business line. Flag any variances outside of +/-10% and assign a manager or lead staff member to provide an explanation of the variance. [4]
Conducting audits (internal or external)	A systematic review of an organization's financial systems, records, and controls to detect errors, inconsistencies, or misuse. External audits are only expected of ESEs in the "Growth" stage of maturity or later.[5] Other types of audits may include periodic informal and internal audits.	An ESE's part-time bookkeeper accidentally records payroll tax payments under general "admin expenses" for 18 months. The mistake isn't caught until an external funder review and disqualifies the ESE from funding consideration.	Use an internal mini-audit checklist on a quarterly basis specifically to check that all restricted funds are used properly and coded correctly.

[3] In this specific example, the "Segregation of Duties" preventive internal control is further reinforced by ensuring that the person doing the reconciliation is not the same person issuing or managing payments. This may not be feasible in smaller organizations where the team is smaller.
[4] Regular, annual budget-to-actual reviews are only expected of ESEs in the "Early" stage of maturity and later. However, ESEs should consider whether more frequent reviews are needed for ESE-wide financials or for specific programs or business lines that may require this type of detective control.
[5] See "Introduction to the ESE Financial Health Toolkit" for guidance on understanding where your ESE may be on the maturity matrix.

Corrective Controls: Correct detected errors and address identified root causes

Corrective controls are actions and procedures taken to fix problems that have been identified by detective controls, such as errors, fraud, or process failures. Their goal is to restore accuracy of financial records, address identified root causes of an issue that occurred, and prevent the issue from happening again.

Table: Corrective Controls

Corrective Control	Description of this control	What a real-life "risk scenario" might look like that this control is intended to correct	What it could look like to implement this control to address this specific real-life "risk scenario"
Staff training	Targeted training provided after an error or issue is identified, to correct misunderstandings, reinforce policies, and reduce the likelihood of recurrence.	A program manager attempts to use restricted grant funds to cover food costs for a non-eligible participant, violating the grant terms. This is detected and prevented by other controls.	The ESE conducts a corrective training session for all program staff on allowable vs. unallowable expenses for each funding stream. They also update their training materials and require new staff to complete a short quiz after onboarding to confirm their understanding.
Making adjustments to journal entries	A correction made in the accounting system to fix previously recorded financial transactions that were entered incorrectly, such as using the wrong account, amount, or class.	The bookkeeper accidentally posts a $5,000 donor gift to earned revenue instead of contributed revenue, skewing DBL analysis and fundraising reports. The error was detected during an informal internal audit.	Upon detection, the Controller enters a correcting journal entry to reclassify the donation into the correct contributed revenue account and annotates the entry with a note explaining the error.
Making updates to existing internal controls	Modifying or strengthening policies or procedures after discovering that an existing control failed to prevent an issue or was insufficient for current needs.	A former employee accessed sensitive payroll records in the accounting system the day after termination; current termination checklists require revoking access within 72 hours.	Existing termination checklists are updated to require revoking system access for terminated employees within 6 hours.