**Summary of Controls**

**Finance Group**

To mitigate the risks posed by material misstatements and fraud, we have implemented controls into the database. These can be split into two areas: system controls and process controls, each playing a role in lowering the risks faced by the company.

**System Controls**

System controls are the first line of defense against any material misstatement. Access allows for various tools we used to combat any incorrect data entry. We have implemented field length verification for standard fields, such as identification numbers, to ensure that the data is properly recorded in the database. In addition, dropdown boxes have been implemented in forms to ensure that no typographical errors can occur in data entry. Several of our queries have type-two outer joins, ensuring that our reporting shows all applicable data even if it doesn’t have a counterpart in the joined table. An example of this is in the Shares Redeemed Query, where all shareholders are shown; those without redeemed shares are shown as having not redeemed any. Finally, with data verification built into the relationships of the database, we have enforced referential integrity, allowing for us to control what is entered in to linked fields; for example, we can ensure that a given dividend is linked to an existing user, is payed from the correct account, and has employee authorization.

**Process Controls**

In addition to the system controls, we have built various controls into the processes themselves. This can be split into two rough sections: change controls and access controls. Change controls consist of who has permission to change either the system itself or the data within the system. We have clearly defined user groups showing who can make changes and what they can change. This also splits users to ensure that segregation of duties is being enforced: for example, an employee purchasing a short-term investment will not be the same one recording the sale of that investment into the system along with the associated gain or loss. To ensure this is the case, various actions require approval from management, and all disbursements that are made must be approved by the Treasurer of the company.

To ensure that the change controls are not circumvented, we have implemented access controls into the accounting system. Each user is given a unique employee ID. They are instructed to create their own unique password, which contains a combination of letters and numbers, both upper- and lower-case, and at least one special character. This password must be changed every 90 days. After 5 incorrect login attempts, the user will have to verify their ID with the IT department.  Each login from a computer is tracked, and should a user login on a computer that is not theirs, the IT department will be aware. Finally, each employee is given a badge to get into the company offices, ensuring that non-employees must sign in to enter the building.

**Auditability**

These controls help to ensure the auditability of the system and the maintenance of a clear audit trail. Referential integrity ensures that the data is consistent across all tables, making it easy for an auditor to follow the necessary steps to verify. Type-two outer joins ensure that no data is missed in the reports being pulled from the system, allowing for easy cross-referencing with source documents. And the various user IDs and approvals throughout the system allows for an audit trail to be maintained and enforced.