

FRAUD AND INTERNAL CONTROLS

FMI

November 23, 2009

Segment 1

Presented by

Everett E. Colby, BSBA, ALA, CFE, FCGA

Colby McGeachy, PC – IMF Porter Hetu International

NEED FOR CONTROLS

- ◆ Many authorities on fraud believe the most important thing an organization can do to deter fraud is design internal controls that make it difficult to commit fraud
- ◆ Internal control systems have to be enforced
- ◆ Internal controls help ensure the accuracy, integrity and safety of system resources

TECHNOLOGY ARMS RACE

- ◆ Technology landscape is constantly changing
- ◆ The race is between those trying to protect systems and those trying to compromise systems
- ◆ Controls to protect systems are developed at a much slower pace than the systems themselves
- ◆ Lag period between technology advancements and control systems is where dishonest people do most damage

TECHNOLOGY ADVANCES

- ◆ Main frames
- ◆ Client/server
- ◆ Internet
- ◆ Electronic commerce
- ◆ PC's
- ◆ Portable computers

THREATS TO INFORMATION SYSTEMS

- ◆ Business is increasingly more dependent on accounting and information systems
- ◆ Information systems have become increasingly more complex to deal with the need for information
- ◆ Controlling the security and integrity of systems has become increasingly more important

NATURAL AND POLITICAL DISASTER

- ◆ The Mississippi and Missouri rivers flooded parts of eight states. Many companies lost computer systems to flood damage
- ◆ Earthquakes in Los Angeles destroyed systems and others damaged by falling debris
- ◆ 9/11 attacks in New York
- ◆ Fire, excessive heat, high winds

SYSTEM FAILURES

- ◆ Bugs in a new tax accounting system blamed for California's failure to collect \$635 million in business tax
- ◆ At Bank of New York, a field used to count the number of transactions was too small to handle volume. Error shut the whole system down and left bank \$23 million short when it tried to close its books
- ◆ Hardware failures, power outages and undetected data transmission errors

UNINTENTIONAL ERRORS & OMISSIONS

- ◆ A data entry clerk at a company mistakenly keyed in a quarterly dividend of \$2.50 per share vs. \$0.25. The company paid \$10 million in excess dividends
- ◆ Bank programmer mistakenly calculated interest using 31 days for each month – over \$100,000 in excess interest paid
- ◆ Accidents caused by human carelessness, failure to follow procedures and poorly trained or supervised staff

FRAUD

- ◆ Systems programmer at bank learns that interest is only calculated to 6 decimal points. Programs to calculate to 7 and excess is automatically wired to offshore account – found guilty after theft of over \$2.5 million US
- ◆ A manager at newspaper went to work for a competitor after being fired. First employer soon realized that its reporters were constantly being scooped on stories. Discovers that former manager still had access and password to computer system

WHY ARE THREATS INCREASING

- ◆ Increasing number of client/server systems means information available to larger number of people
- ◆ Because LAN's and client/server systems distribute data to many people, they are harder to control
- ◆ WAN's are giving customers and suppliers access to each other's systems and data

WHY COMPANIES DO NOT HAVE BETTER DATA PROTECTION

- ◆ Computer control problems are often underestimated and downplayed
- ◆ Companies view loss of crucial data as a distant, unlikely threat
- ◆ Control implications of moving from centralized host-based system to networked systems are not fully understood
- ◆ Many companies don't realize that data security is crucial to their survival
- ◆ The benefits are not seen to outweigh the costs

IMPORTANCE OF DATA

- ◆ Data is a strategic resource
- ◆ Protecting it should be a strategic requirement
- ◆ Many companies would fail if mission critical data was not available for a short period of time
- ◆ Data can be very valuable to competitors – client lists, new product designs, pricing schedules

DESIGNING CONTROLS TO CURB THE THREATS

- ◆ Many companies are becoming more proactive in their approach
- ◆ More companies are educating their employees about control measures
- ◆ Establishment of formal information security policies by making controls part of applications development process
- ◆ Movement of sensitive data off unsecured servers to a more secure environment like mainframes

DESIGNING CONTROLS TO CURB THE THREATS

- ◆ Overall responsibility for a secure system lies with top management
- ◆ Although internal control objectives remain the same regardless of data processing method, computer based systems require different policies and procedures
- ◆ Segregating duties in a computer system is more difficult than in traditional environment