Internal Controls

Fin 0100
Welcome to this online class on internal controls.

My name is Andy Zell, Business & Reporting Analyst in the Controller’s Office, and I will be your online instructor.

Before we begin, please download and print the worksheet entitled “Internal Controls”

At specific times during our class, you will be instructed to use this worksheet.

Ready?

Let’s begin.
This class will discuss the importance of internal controls for employees here at Stanford. Although at times we will be referring to the manager’s role in implementing internal controls, internal controls are everyone’s concern.

At the end of this class you will know:

1. What internal controls are, and
2. Why internal controls are important

...so that you can
1. Identify weaknesses and risks for your areas of responsibility.
2. Assess those risks, and
3. Determine the controls needed.
All organizations have goals and objectives.

Businesses deliver goods and services to realize a profit. When businesses do not adequately anticipate and mitigate risk, they can run into big problems which affect not only their business but their clients and the world around them.

Take Jack in the Box, for example. When their food handling operations failed, people got sick and some even died of E coli poisoning.

When the leaders of Enron colluded to defraud the company, they ruined the company and the financial security of thousands of employees and stockholders.

And the decision by Hewlett Packard’s Board Chairwoman to illegally spy on other board members to prevent information leaks created both a compliance and a reputational risk.
Colleges and universities also have organizational goals and objectives around their central mission to teach and to conduct research. When colleges and universities do not adequately guard against the risks to their mission, they can run into trouble in a variety of ways:

In 2004, auditors recommended that the University of Southern California reimburse the government for costs deemed improper related to an HIV-education project for violations of human subjects in research procedures. The recommendation was the result of inadequate adherence to federal regulations -- a compliance risk.

In 2006, an audit of the University of California revealed that the President of the University had been awarding non-monetary benefits to new senior executives over a nine year period without informing the board. The undisclosed amounts were estimated to be in the hundreds of thousands of dollars.

In 2004, a lawsuit filed against Princeton University for misuse of donor gifts placed the University’s reputation at risk among its donors.

All organizations must control the risks that threaten their organizational goals.
Even at Stanford, there have been problems resulting from lapses in internal controls. In the 1980’s and early 1990’s inappropriate indirect cost charges to the federal government were discovered for expenses like a 72-foot yacht, the upkeep of the Stanford family mausoleum, and the cost of furniture for the University president’s residence. The discovery of these charges resulted in a US Department of Justice investigation that lasted over two years.

Even though no fraud was found, the news reports, editorial cartoons, and talk show monologues triggered by the embarrassing accounting and control errors seriously damaged the University’s reputation. Additionally, the investigation cost Stanford over $25 million for outside accounting firms and consultants to provide independent verification and to assist with its response to the Government’s allegations.
In business, the *processes or activities* that provide reasonable assurance that an organization will meet its objectives are called...
Internal controls.

Internal controls are business practices that provide assurance that an organization will achieve its goals.
It is every employee’s responsibility to safeguard the University’s assets. Stanford is a very busy place. In such a highly decentralized and diverse institution like Stanford, it is especially important that all employees are vigilant.
Employees ensure that the system works by:

- Identifying operational risks
- Executing internal controls
- Analyzing discrepancies and questioning unusual items

Most problems are discovered by attentive and alert employees. For example, when student loan documents sent to an academic office at 5PM on a Friday were promptly returned, signed, at 8 AM the following Monday, it amazed a Student Service employee. How did the returning agent find all ten students and secure their signatures so quickly? The astute employee called in supervisors. Sure enough, the signatures on the loan documents did not belong to the 10 students. Thanks to that alert employee, a fraud was prevented.
Everyone needs to be able to identify potential risks within their areas of responsibility. If you are a manager, it is your responsibility to identify the potential risks to your department’s goals and implement procedures and policies to mitigate those risks. If you are a staff member, you can help your managers by bringing possible risks and control concerns to their attention.

The Internal Controls Framework, developed by the Committee of Sponsoring Organizations (COSO), can help. It identifies the 5 components of the Internal Control System:

1. Control Environment: *What is the culture of the organization?*
2. Risk Assessment: *Where can things go wrong?*
3. Control Activities: *What can we do to avoid problems?*
4. Monitor: *Is it working?*
5. Information and Communication: *Is there an open and effective channel of communication?*

You can use this framework as a guide to ensure that your department is implementing the internal controls appropriate for your area of responsibility.
The foundation of the Internal Control framework is the Control Environment.

The values of an organization and the way those values are modeled by its leaders set the tone for the entire organization.

If the leaders of an organization do not model consistent, conscientious and ethical business practices, the entire enterprise is at risk of failing. The problems of the Enron Corporation, for example, stemmed from corrupt leaders who colluded to defraud the company.

At Stanford there is a Code of Conduct that sets the tone and the guidelines for employee responsibility and behavior. Integrity and quality, conflicts of interest, compliance with laws and regulations are articulated in the University’s Code of Conduct.

Leadership takes place at all levels of an organization. If you are a manager at Stanford, no matter how small your department is, you are a leader and you are responsible for setting the tone for your organization.
There are many attitudes and behaviors of an effective manager.

Do you or does your manager:
Empower employees to take initiative and point out potential problems?
Model desired behavior like admitting mistakes and asking for help?
Work collaboratively by openly discussing issues and concerns?
and
Support employees through on-going training?

These are just a few examples of the kinds of behaviors and attitudes a good manager will model to create a positive control environment for his/her team.
The pursuit of every goal and objective is associated with risks.
A critical aspect of maintaining control is to:

Identify
Assess, and
Analyze

...the risks associated with your area of responsibility.

It is important to determine:

1. What could go wrong?
2. The likelihood that it will go wrong, and
3. The associated cost of preventing the risk vs. correcting the error later

These are the considerations in Risk Assessment.
There are 5 categories of risk: financial, operational, compliance, reputational and strategic.

Financial Risks are risks that have to do with the loss of money.

Operational Risks are risks that arise from poorly conceived or poorly executed processes. Restaurants, for example, have the goal of serving their customers delicious and safe food. In the E coli case which affected Jack in the Box, certain operational processes placed that goal at risk.

Compliance Risks are risks that arise from not following applicable laws, policies or applications. Recently, the University of Southern California lost several million dollars in federal funding because they did not comply with federal standards regarding human subjects in their AIDS/HIV research grant.

Reputational Risks are risks that damage an organization’s reputation. In 2007, JetBlue held hundreds of passengers in airplanes on runways for over nine hours waiting for weather to clear. For an airline that espouses superior customer service, this decision put their corporate reputation at risk.

Finally, there are Strategic Risks to an organization’s success. These are risks that result from a business goal that might be unattainable. The dot-com craze was filled with examples of poorly conceived new businesses. The strategic plans for these companies -- the products or services they delivered, or their management plans -- were strategic liabilities that caused them to go belly up.
So, how do you assess risk for your areas of responsibility?

The first step is to identify your goals and objectives.

For example, your top objective might be to manage a sponsored project for a Principal Investigator. Another objective might be, “To maintain a sufficient inventory of laboratory chemicals and supplies.”
As practice, let’s do a Risk Assessment exercise that applies to your area.

Turn to your worksheet now.

You have many goals to accomplish in your job. Choose one of your goals and write it on the goal line of your worksheet. In our example, a top goal might be to “Manage a sponsored project for a Principal Investigator, or ‘PI.’”

You can pause the audio narration by clicking on the PAUSE button at the bottom of the screen while you work this part of the exercise. Click the PLAY arrowhead to resume the class when you are ready.
The next step in the process is to identify the risks that could prevent you from achieving your goal.

**Steps to Assessing Risk: Identify Risks**

1. Identify Goals/Objectives
2. **Identify Risks**
3. Prioritize Risks
4. Plan Control Activities
Now that we have identified the 5 categories of risk, let’s return to our Risk Assessment exercise.

Think about your stated objective. What kinds of risk exist for you area? Do you have Compliance risks that threaten your objective? What about Financial, Operational, Reputational or Strategic risks?

Next, what assets do you need to protect? Are you responsible for securing cash, equipment, information (Social Security numbers or salary), reputation, land, or people?

What significant changes have occurred recently? Are there any new technologies or laws, that you need to consider? What about cost pressures or staff turnover? All of these represent considerations that must be monitored periodically to make sure new risks have not developed.

Finally, how much would it cost to control the risk?
In the example on our worksheet, one of the risks involved in managing a sponsored project for a PI is a financial risk: *Improper expenditures could be charged to the sponsored project (e.g., unallowable, unauthorized, or not applicable to the project).*

Take a moment to fill in your worksheet with the top 2 or 3 risks to the goal you have selected.

On your worksheet, write down some of the risks that may threaten your ability to achieve your stated objective.

**PAUSE** the audio to work on the exercise. Click the **PLAY** arrowhead when you are ready to resume the class.
Once you have identified the risks associated with your area of responsibility, you need to prioritize them.

Let’s look at how to do that.
In prioritizing risk you need to consider:

What are the **consequences** of each risk?
Could the consequences of a risk result in fines or lost revenue?
Could a risk result in the loss of a donor or sponsor?
Could we lose a prestigious faculty member?

What is the **likelihood** of the risk occurring?
Is it remote or is it highly probable?
And...
What is the **cost** of the control?
Even more important, can the problem even be mitigated or corrected after the fact?
It is important to consider how that cost compares to the cost of correcting the error later.

Finally, remember that the **cost of the control should not exceed the cost of the benefit**.
In summary, risk assessment is an important feature in the Internal Control Framework.

It involves:
Identifying your goals and objectives
Identifying the risks to each of your goals and objectives by understanding the 5 categories of risk
and
Asking the right questions.

You cannot control every risk. Therefore, you need to prioritize them against the consequences, the likelihood of the occurrence, and the associated costs.

We hope these steps help you understand how to assess risk. Now you can perform this analysis for other objectives in your area of responsibility.
Let’s refer back to our exercise. Take a moment to prioritize the risks. Using a scale of 1-5, where 1 is low and 5 is high, give each risk you have identified a score for Consequence of risk and Likelihood of occurrence.

For the purpose of our Risk Assessment exercise example, we’ll prioritize the Consequence for our first risk. We think that the consequences of improper expenditures are very high, so we rate that risk as a “5”

Let’s assume we believe the chances of an expenditure being mischarged, for whatever reason, are relatively high, let’s rate likelihood as a “4”.

Since the Cost column pertains to the cost of controls, we will complete this column after the next section.

**PAUSE** the audio to work on your exercise. Click the **PLAY** arrowhead when you are ready to resume the class.
The policies and procedures you design and execute to mitigate risks to your goals are called “control activities.”

Now that we have identified and prioritized our risks, it is time to set up control activities which can mitigate those risks.

There are two categories of control activities: Preventive and Detective

Preventive controls are designed to identify an error before it occurs. For example, approvers should review transactions for propriety, appropriateness and proper coding before they sign off and the transaction is recorded in the financial records.

Detective controls, on the other hand, identify errors after they occur. Reviewing transactions on reports is a detective control, as this process will only identify errors after they occur.

Both preventive and detective controls are effective. Specific circumstances will determine which to use.
For every identified risk, there are many possible controls.

Among the most important controls for mitigating Financial and Operational Risks are:

Segregation of Duties
Securing Assets
Reconciliation, and
Review of Reports
Segregation of Duties insures that no one person has complete control over a transaction.

There is a lot of misunderstanding about segregation of duties. It is not just an accounting procedure, it is good business practice. Segregation of duties, or having “a second pair of eyes” authorize and record transactions, is a critical control in mitigating financial risks.

The purpose of a second pair of eyes is to divide responsibilities among different people to reduce the risk of error or inappropriate actions.

For example: The person who approves the purchase should not be the one who receives the asset, records the transaction and reviews the expenditure statement.

It should be noted that some departments are too small to achieve appropriate segregation of duties for each individual transaction. In these cases, to protect both the University’s assets and the department employees, periodic reviews by higher level management or an independent party should occur.
Securing University assets to prevent theft is a prime example of a preventive control. If you are responsible for equipment, particularly laptop computers, you should have a system for securing them.

In June of 2008, a Stanford laptop, containing personal data for approximately 62,000 current and former employees, was stolen. Stanford mobilized to contact the affected individuals, sending notifications to current & former employees. Stanford also hired a risk-consulting company to provide one year of credit reporting, credit monitoring, and identity restoration services, at university expense, for any affected employee who wished to sign up. This incident was costly, not only in dollars, but in potential risk to employee information and to the public trust.

What controls do you have in place to secure laptops?

If you are responsible for cash and collecting checks, you need to be sure to lock your cash, and deposit checks immediately. When you can’t deposit checks immediately, make sure they are locked up, too.

Do you have clearly communicated guidelines for protecting the assets for which you are responsible?
Physical assets are not the only assets that need securing. Information can be lost or stolen as well.

Colleges and universities have significant sensitive data assets such as social security numbers, student data and donor information. Data loss can occur through human error or as the result of criminal intent. Hackers have breached the computer networks at dozens of major universities, often trying to access social security numbers of students. Ohio University recently revamped their IT protocols after hackers gained access to their computer system and the personal information for over one hundred and thirty thousand students. San Diego State’s financial aid records were broken into exposing the vital information of thousands of students. These are but two examples of data security incidents that occur regularly at colleges and universities.

Computer passwords and back up systems are among the controls that you can implement to safeguard information.

Remind your team not to share their passwords and to change their passwords frequently.
Reconciliation is the process of comparing the entries on key reports to supporting documentation and resolving any discrepancies.
This is done:
To ensure the accuracy and completeness of transactions in the University’s financial system,

To ensure inappropriate changes or charges did not occur,

And

To resolve discrepancies in a timely fashion.

A critical procedure in performing reconciliations correctly is to use source documentation when validating transactions. For example, a purchasing transaction should be validated by an invoice from the vendor.
In addition to Reconciliations, every department at Stanford is required to conduct a monthly review of their financial information reports.

Reviewing reports is a troubleshooting process in which you examine current results against your budget, and ask questions like:

- Are expenses allowable under Federal regulations, University policy, and fund restrictions?

- Are the expenses reasonable? Would someone purchase and pay this much for the good or service?

- Is there anything unexpected?

- Are there trends or problems?
Now that we have discussed control activities, let’s return to your Risk Assessment worksheet.
In our exercise example, possible control activities for preventing improper expenditures might include: Approval of a purchase transaction, reconciliation of the PTA, and review of the PTA.

Look at each of the risks that you have listed on your sheet. Write down some control activities that would mitigate each one.

Now, estimate the relative cost of implementing each of these controls, again using a scale of 1 to 5 where 5 is high. Compare the cost of the controls to the cost and likelihood of the consequences previously identified. For example, if the likelihood and consequence of a risk are high, you may decide to implement higher cost controls than would be reasonable if the likelihood of a bad consequence were low.

Risk assessment can be a complicated and subjective process. This exercise was designed to help you begin to analyze risks and tradeoffs in your operations. When faced with situations where both the cost of the consequences and the cost of the controls are high, you may want to use dollar values in your analysis.

**PAUSE** the audio to work on your exercise. **Click** the PLAY arrowhead to resume.
Here are some other Control Activities to consider:

Training: Teaching employees how to perform necessary procedures and keeping their skills and knowledge current

Approvals: Supporting documentation has been reviewed by someone assigned to approve them and they are satisfied that the transaction is appropriate

Documented policies and procedures are the written information that sets forth rules, guidelines, or instructions on how to perform a task.
Now that you have successfully identified your goals and their associated risks and implemented control activities, the next step in the Internal Control framework is to monitor your system.

The control process must be monitored and modified as necessary.

The key is to be vigilant in implementing and maintaining appropriate control activities. Remember: Just because a control activity has not identified a problem or an error in a while, does not mean that that risk does not exist and you don’t need the control.

As a manager, you should monitor internal controls by asking yourself:

Is the control adequately designed?
Is it being properly executed?
Is it effective?
Are there new risks that need to be assessed?
As new situations arise and strategies change, it is important to keep information flowing across, up and down the organization so that you can adjust and correct the internal control framework.

For example, staff turnover or changes in policies or laws may trigger new risk analyses or implementation of new control activities.
Remember: It is every employee’s responsibility to safeguard the University’s assets and mission.

Every manager must be vigilant in establishing the internal controls framework for his or her department.
At the end of every fiscal year, as part of our annual audit, managers from key University departments attest to the maintenance of internal controls in their departments.

These representations are a collective promise that everyone at Stanford is following internal controls to mitigate the risks to the University’s mission and reputation.
To the best of our knowledge, there are no significant deficiencies in the design or operation of internal controls within the School or Department that would be reasonably likely to adversely affect the University’s ability to record, process, summarize and report financial data.
So, now that you have an understanding of what internal controls are and why they are important to you at Stanford, you may need some additional help and resources.
Here is a checklist that you can use to Get Started with Internal Controls.

Take a minute to read it over.
Here is a list of resources that will help you assess and implement internal controls. You can click on the hyperlinks to view and bookmark these web pages for your future reference.
The University has other resources to help you with internal controls.

If you need advice or consultation, email Sue Schmitt, Associate Controller, in the Controller’s Office.

The Office of Institutional Compliance can help with questions or concerns that employees have regarding policies and procedures. A "Helpline" form is available to provide reporting of non-compliance (anonymously if you wish) or to ask questions regarding compliance.


If you would like additional training, there are 2 courses you can take, Cost Policy and Chart of Accounts and Reconciling and Reviewing Expenditure Statements. You can register for these courses using STARS.
This concludes our online class on internal controls.

We hope this has given you the information you need to review and assess your department’s internal controls.

To receive credit for this course you must complete the course exercise.