IOWA STATE UNIVERSITY

Office of Internal Audit

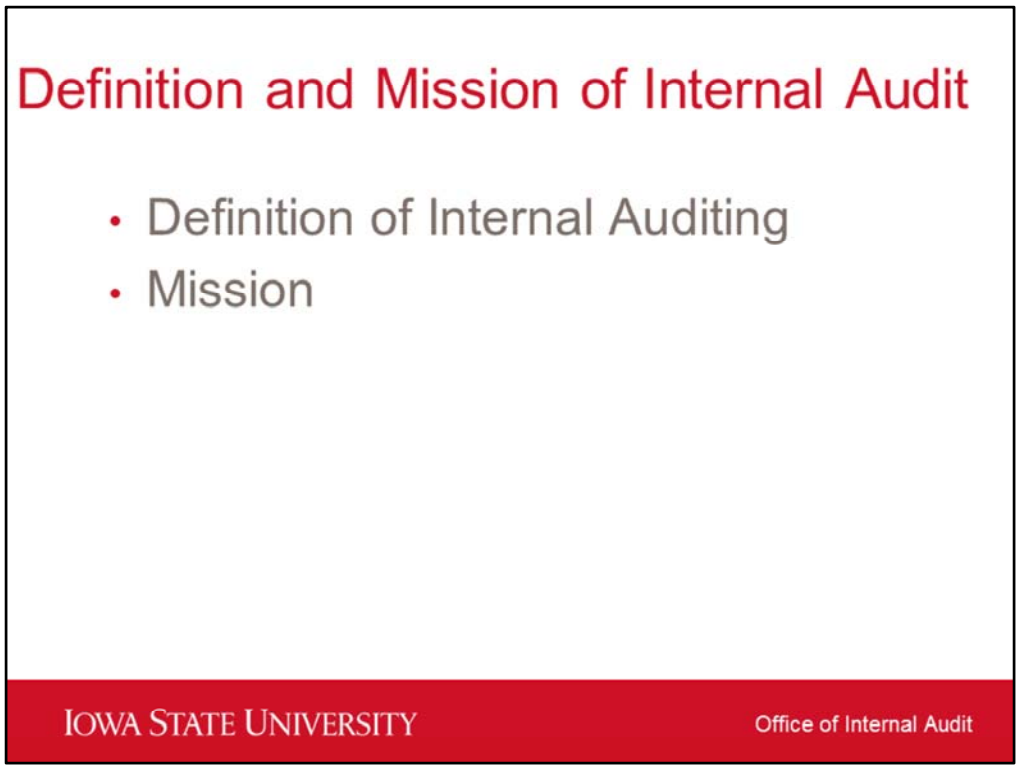
Office of Internal Audit
September 15, 2016

Presented by:

Jordan Bates, Audit Manager

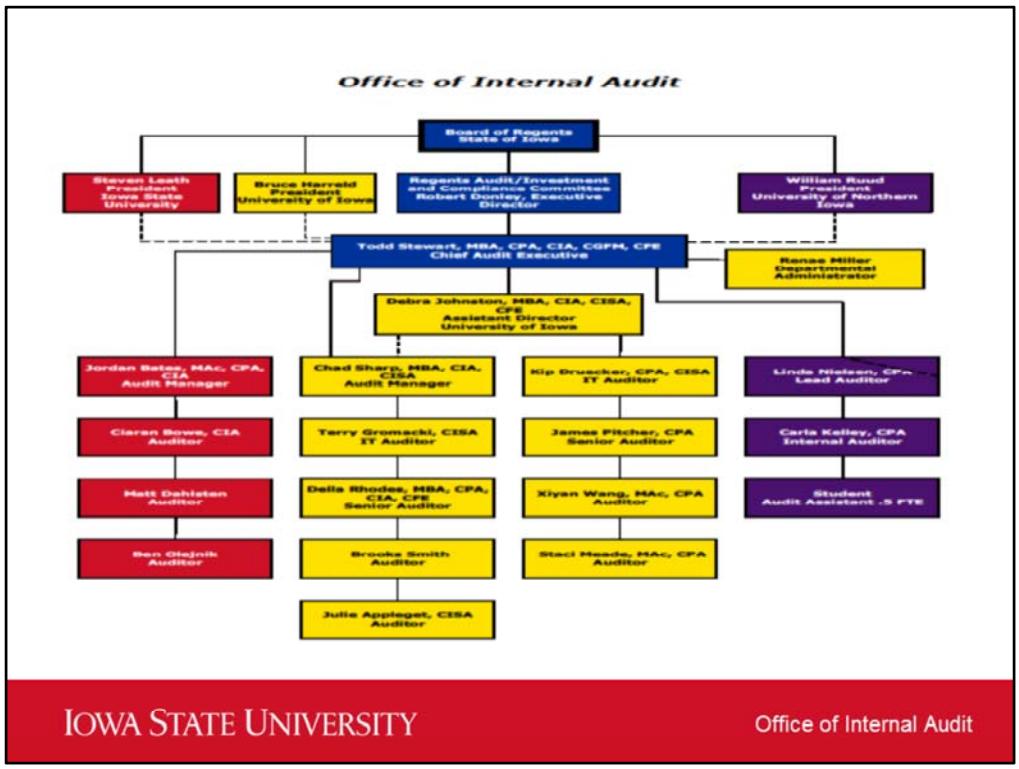
Presentation Overview

- Definition of Internal Auditing
- Internal Audit Function at ISU
- Audit Plan Determination
- Common Findings



Internal auditing is an independent, objective assurance and consulting activity designed to add value and improve an organization's operations. It helps an organization accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control, and governance processes.

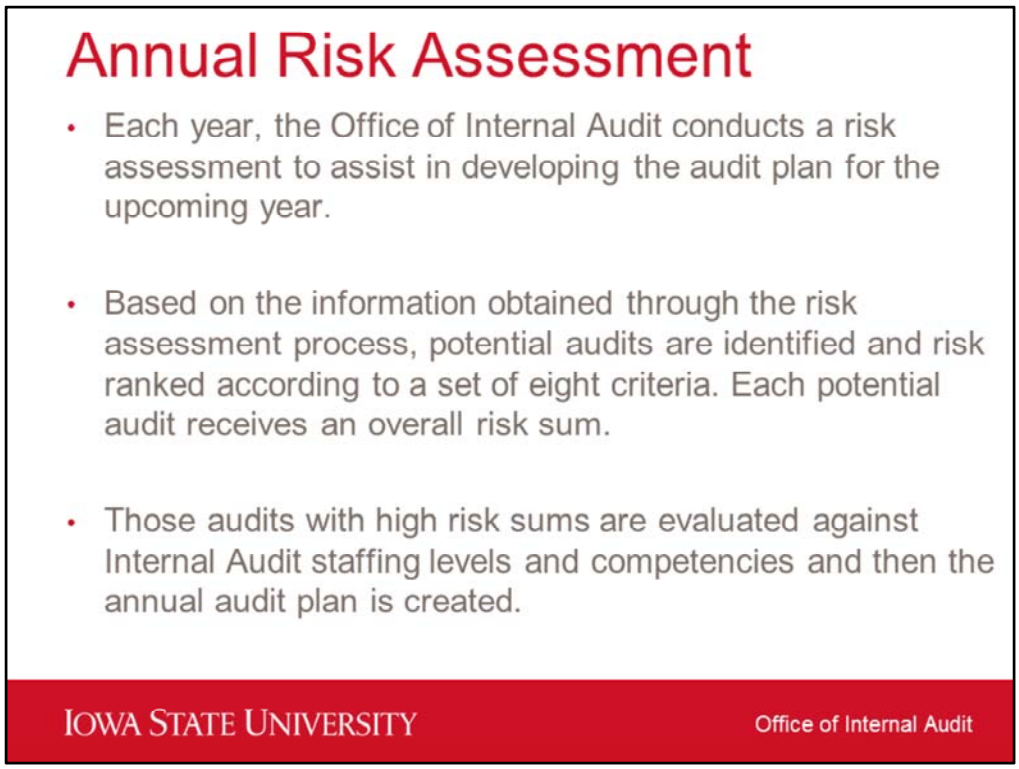
The mission of Internal Audit is to partner with management to enhance and protect organizational value by providing an independent and objective assessment of operational efficiencies and controls.



In the state of Iowa, the internal audit function is a consolidated function. That means that the three regent institutions share a Chief Audit Executive, but also maintain their own local audit staffs.

At each institution there is a dual reporting relationship. There is a functional reporting relationship to the Audit/Compliance and Investment Committee of the Board of Regents, State of Iowa. There is also an administrative reporting relationship to the President at each institution.

Internal Audit authority is granted through the Internal Audit Charter which is approved annually by the Audit/Compliance and Investment Committee of the Board of Regents, State of Iowa. It was actually just reapproved last week at the Board's September meeting.



The risk assessment consists of a series of interviews with senior leaders and administrators across campus (approximately 40 meetings).

This past year, we tried out something new and conducted three online surveys to some targeted groups of individuals based on their roles and responsibilities within the organization.

Risk criteria includes:

- Impact on the University mission
- Financial significance
- Legal/regulatory environment
- Level of change
- Information security/technology
- Reputational risk
- Complexity
- Control environment

The audit plans of the three regent institutions are presented by the Chief Audit Executive during the September meeting of the Audit/Compliance and Investment Committee of the Board of Regents, State of Iowa. In this meeting, the audit plans are reviewed and formally approved.

While all internal audits are going to have different objectives, there are some processes that we would typically be considering that lead to some common findings.

Some of these relate directly to sponsored programs and some of them may be more tangentially related, but it may be you handling these processes for your department or unit or it may be someone you work with directly.

In terms of sponsored programs, departments are responsible for maintaining certain documentation. What we have found throughout audits, is that departments may not be consistently retaining:

- Award Documentation
    - This is important so that those departmental administrators responsible for approving expenditures can refer to award documentation in real time at the time of the approval to determine if purchases are allowable.
- Principal Investigator approval of subrecipient invoices
    - As the prime recipient of an award, Iowa State University is responsible for monitoring the programmatic and financial activities of its subrecipients in order to ensure proper stewardship of federally sponsored funds. Principal Investigators must review invoices to ensure the incurred costs follow the subrecipient's approved budget and ensure that costs are reasonable per the amount of work performed. This review must be documented in one of three ways:
        - The Principal Investigator directly approves the subrecipient's invoice in the VO system.
        - The Principal Investigator signs a copy of the subrecipient's invoice and forwards it to the departmental administrator and this documentation is retained.
        - The Principal Investigator emails the departmental administrator indicating approval to pay the invoice. Although not required, I'll add here that if this is the method selected, we would recommend that the departmental administrator PDF this email approval and add it as an attachment to the invoice in the VO system. That way the invoice and approval are all in one place.

In terms of travel on a sponsored program, the benefit to the project may not be adequately justified in business purpose. I'd pay attention for this regarding attendance at a conference. A business purpose of "attending ABC conference" would not be adequate and does not detail how attendance at this conference benefits the project. An adequate business purpose would say something along the lines of "attending ABC conference to present or distribute research results regarding XYZ project."

Iowa State University encourages active participation of university personnel in external activities that promote the university's mission, enhance professional skills, expand knowledge, and/or contribute to public service. At the same time, the university expects all employees to have an allegiance to the university and to guard against possible adverse effects of their activities on the performance of their university duties and the reputation of the university.

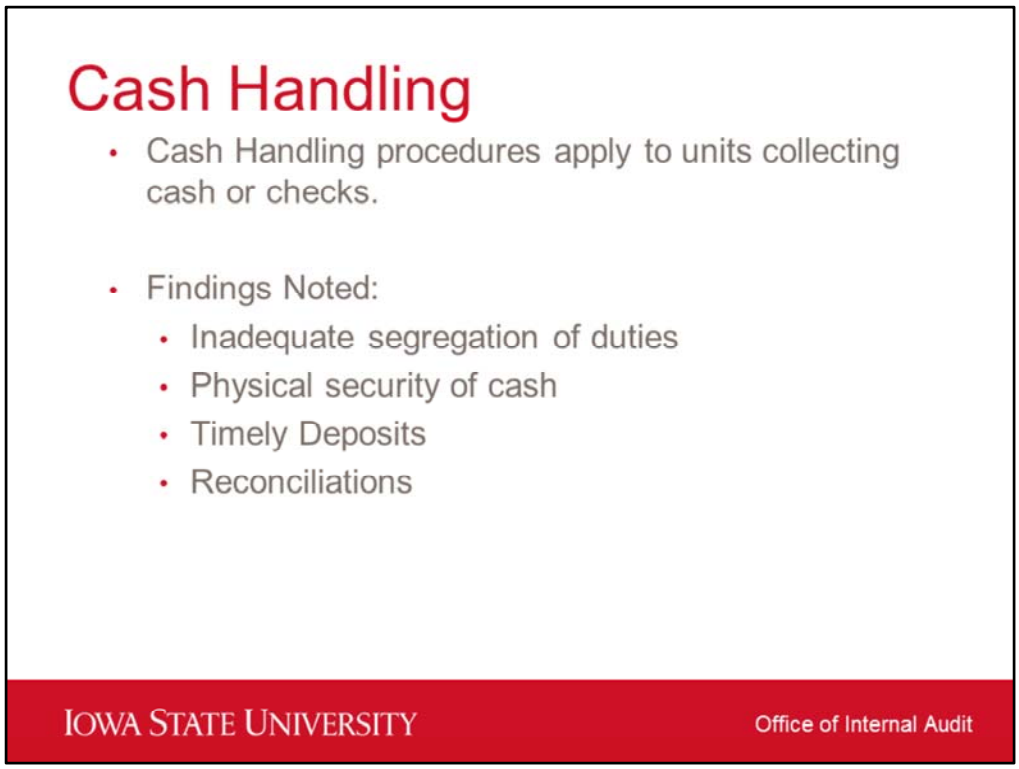
Within the last several years, I think that as an organization, we've really seen the disclosure rate increase as more and more faculty and staff are aware of the policy, but this is something we need to stay on top of as the level of engagement in activities may change rapidly. We can't actively manage the conflicts that we don't know about.

What we're seeing more of now is not getting the disclosure completed a the beginning of employment, depending on the time of year that an employee is hired, they could go virtually a year before disclosing. Adding this to an onboarding checklist helps ensure this is completed for new employees. Also, C Base employees, graduate assistants are required to disclose and this can be difficult in communicating and obtaining. Departments can incorporate this into graduate assistant onboarding and communicating to major professors that their graduate assistants should be completing disclosures.

The unit may not have properly developed their rates for fee-for-service operations. Internal customers should be charged at cost. External customers should be charged at least cost + the administrative fee up to the market rate for the service. You should not see cases where external customers are being charged less than internal customers. Also, the rates should be reviewed annually and adjusted as needed.

Only expenditures related to the fee-for-service operation should be charged to the fee-for-service account.

Except for Point-of-Sale transactions, all charges should be processed through university Accounts Receivable. The department should send a separate invoice if an itemized invoice is necessary, but it should note an official statement is coming from the university.



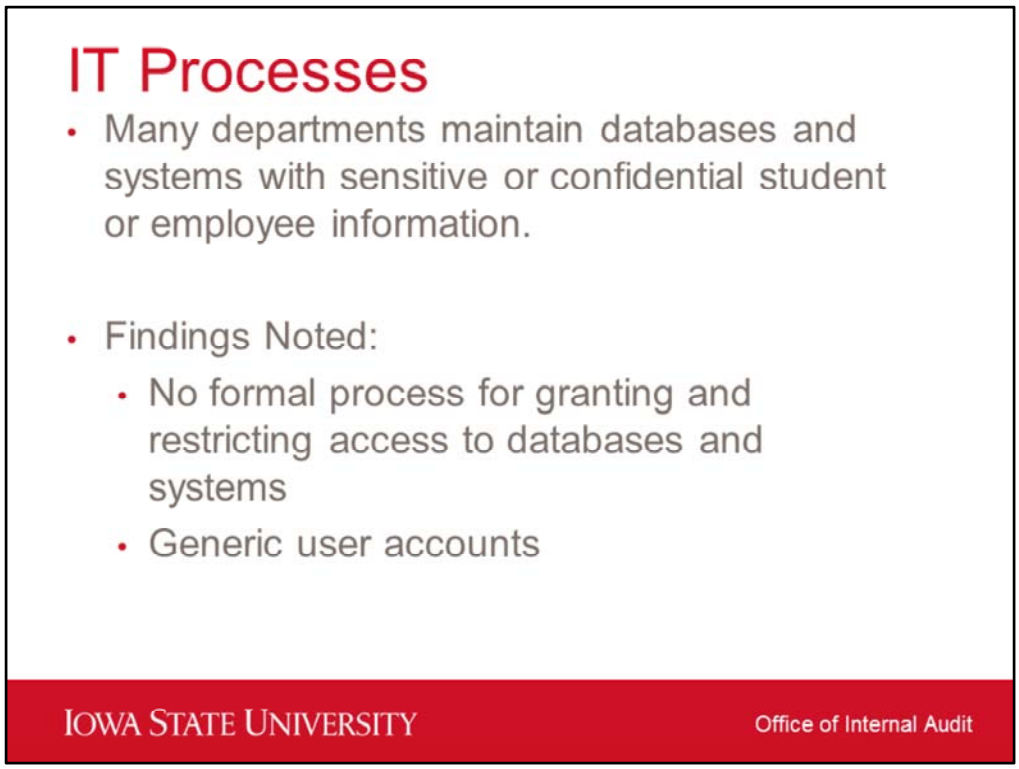
The amount of cash handled varies greatly from department to department. Any department that receives cash or checks from students or the public must follow cash handling procedures established by the Treasurer's Office.

Often an individual has too many responsibilities in the cash handling cycle. Collecting, counting and balancing, and the reconciliation should be performed by separate individuals. Obviously smaller units may have some difficulties with segregation of duties and those units must make a judgment regarding the best separation of duties and any compensating controls that may be needed to help mitigate risks.

Cash should be stored in a locked cash box or safe. Access should be restricted to only those requiring access and combination locks should be changed periodically or when somebody leaves the department.

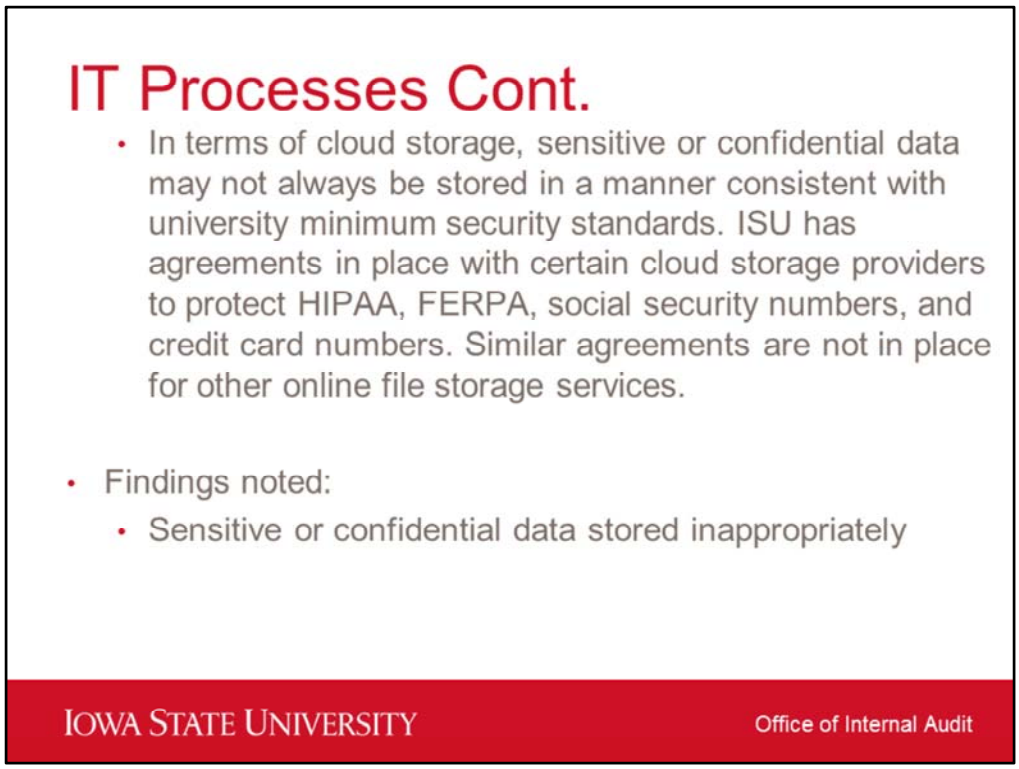
Cash should be deposited within five days when receipts are less than $100 and within two days when receipts are more than $100. Units have a tendency to hold onto cash for a month or until they receive all the cash they were expecting for a specific activity. Cash and checks shouldn't be held by the unit and need to be deposited.

Reconciliations should be performed to compare cash collected to cash deposited by an individual with no other cash handling responsibilities.



Many departments maintain databases and systems with sensitive or confidential student or employee information – admissions/financial aid/scholarships/grades/etc. Some findings noted include:

- No formal process for granting and restricting access to databases and systems. There should be a process in place to approve the access ensuring that the individual requesting the access has a business need for the access. There should also be a process in place to periodically review who has access and if each user still retains a business purpose for needing the access. A lack of user access controls may result in unauthorized access to sensitive or confidential data.
- Generic user accounts – accounts to databases and systems containing sensitive or confidential information should be tied to a specific individual. Accounts utilized by multiple users decreases the ability to trace actions to a specific individual.



Finally, in terms of cloud storage sensitive data may not always be stored in a manner consistent with university minimum security standards.

ISU has put into place agreements with certain cloud storage providers to protect HIPAA, FERPA, social security numbers, and credit card numbers. (CyBox/Microsoft OneDrive)

Similar agreements are not in place for other online file storage services so you want to be careful with what information you are storing and where. (DropBox)

Always feel free to contact the Office of Internal Audit with any questions as we are here to help!