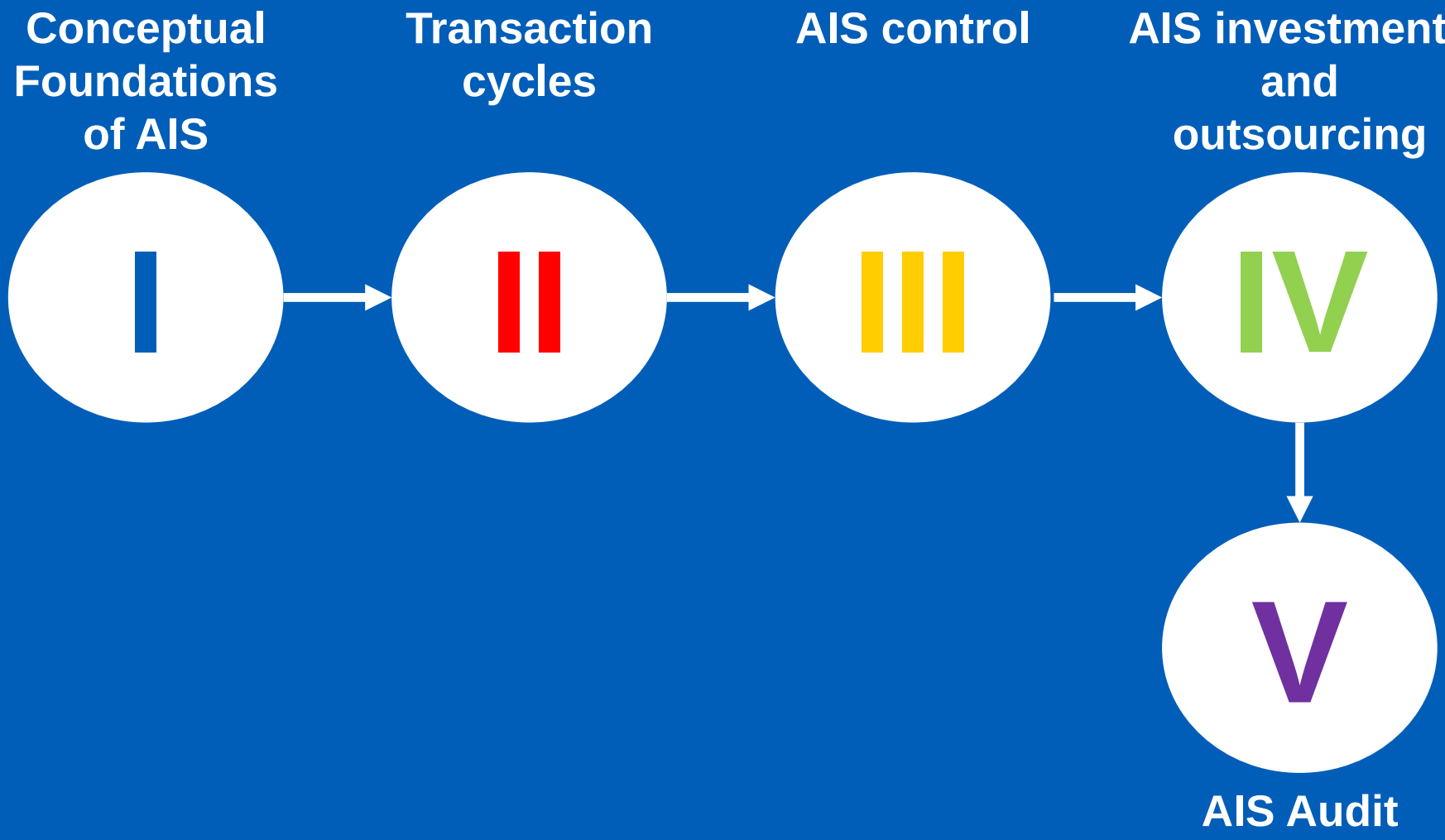
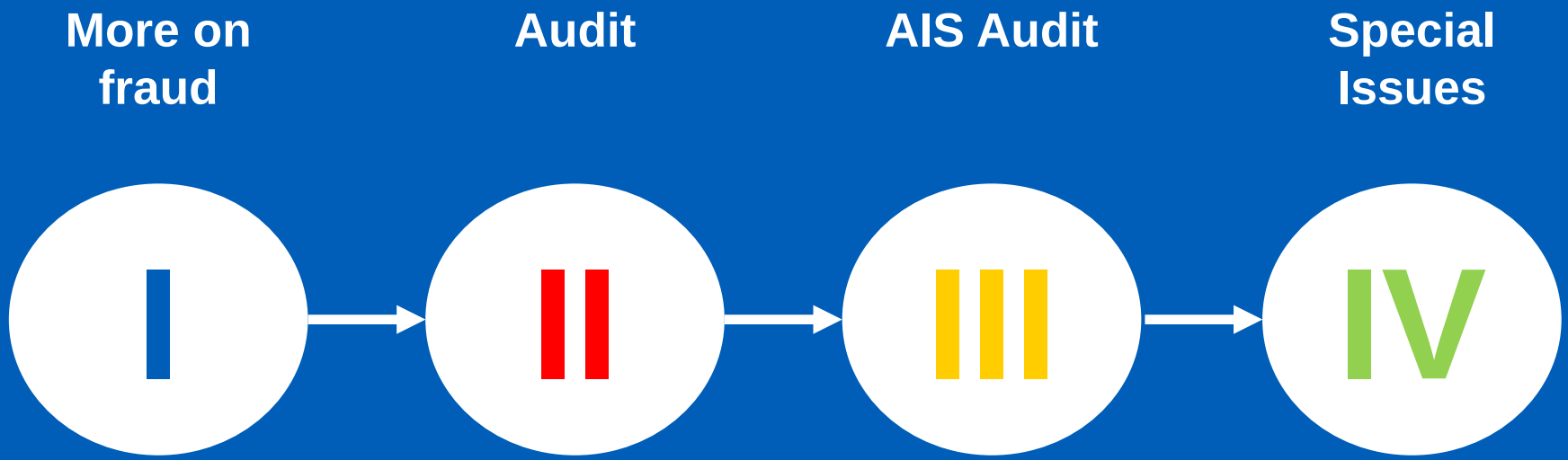

Conceptual Foundations of AIS
Transaction cycles
AIS control
AIS investments and outsourcing
I
II
III
IV
V
AIS Audit

Aalto University
School of Business

AIS (Internal Control) Audit

by David Derichs ©
Lecture 5


More on fraud
Audit
AIS Audit
Special Issues
I
II
III
IV

I. More on fraud

The history of fraud

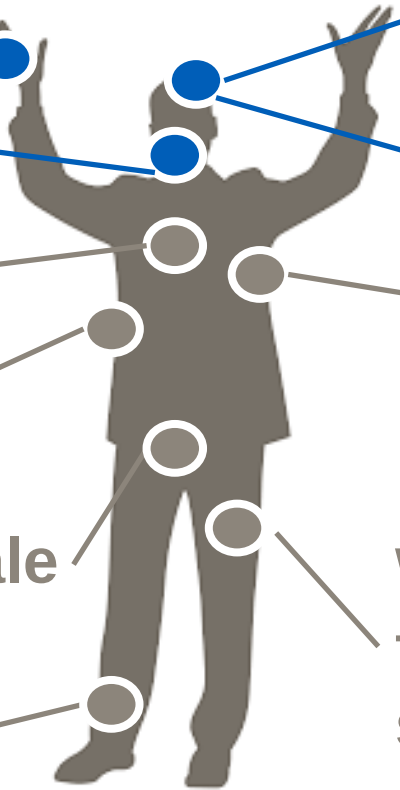
- **Lambroso** (17th century) and **Hooten** (1939) postulating **anthropomorphic indicator**
- 1939, **Sutherland** propagating **differential association** – Focus on crime of **‘respectable people’**
- 1953, **Cressey** introduced the theory of ‘**trust violators**’ and developed the **fraud triangle**
- 1986, **Cornish** and **Clarke** publish the reasoning criminal, introducing the **rational choice perspective**

Non-scientific, but still often circulated theories…

- **Bondsman's hypothesis** arguing that the **'sweet life' has a greater allure** to some people **than honest work** can provide for
  – resonates with a recent KPGM study quoting **greed** as main reason
- **Auditor's assumption** claiming that **'the seeds of crime are in each of us'**
  – Resonates with the fraud tringle notion

Who is a fraudster?

The ‘typical’ fraudster:



Autonomous

Good at lying

86% involve management

68% acted independently

85% male

No prior criminal record

Intelligent and skilled

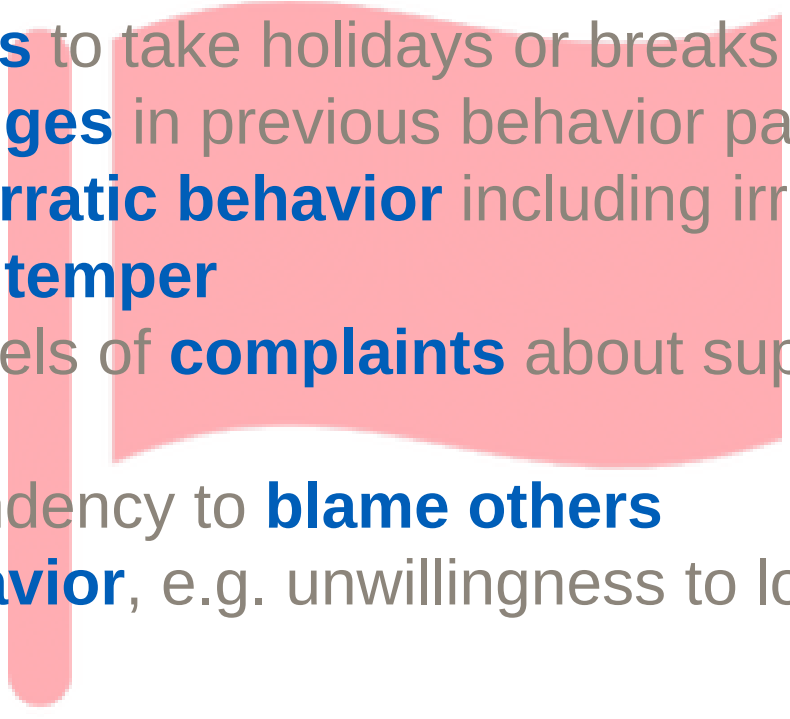
Mentally tough

76% between 36-55 years

Works most often at finance, operation/ sales, then as CEO

Hidden in pre-lecture version

Look for red flags to identify fraudsters



1. **Unwillingness** to take holidays or breaks
2. **Sudden changes** in previous behavior patterns
3. Increasingly **erratic behavior** including irritability and **shortness of temper**
4. Increasing levels of **complaints** about superiors or the organization
5. Increasing tendency to **blame others**
6. **Evasive behavior**, e.g. unwillingness to look people in the eye

Let’s look at a brief case…

II. Audits

What is auditing?

An audit is the evaluation of a system, organization, process project or product

- **Auditing** is the process of **obtaining** and **evaluating evidence** regarding assertions **about economic actions** and **events** in order to determine how well they correspond with established criteria. In practice this means:
  1. an **economic event or action has occurred** (e.g., financial transaction)
  2. what **established criteria exists** for this event? (is it government compliance or regulation? e.g., Generally Accepted Accounting Principles)
  3. how well does this **evidence fit with the criteria?** (e.g., if it's a sales event does the evidence (sales contract) show that the sale was recorded according to IFRS?)

Hidden in pre-lecture version

Assertion	Audit Objective
Existence/ Occurrence	Determine that recorded transactions, events, and related account balances are real and have been properly authorized.
Valuation and Allocation	Determine that recorded transactions and related account balances are • Accurate in terms of dollar amounts and quantities, and any related allocation • adjustments are properly recorded • Supported by detailed evidence • Correctly summarized and posted to the general ledger • Recorded at estimated realizable values
Cutoff	Determine that recorded transactions and events have been recorded in the proper time period.
Complete-ness	Determine that all existing transactions and related accounted balances are recorded—i.e., that none have been omitted.
Rights and Obligations	Determine that transactions and related asset account balances are actually owned. Similarly, determine that liability account balances represent actual obligations.
Classifi-cation and Presentation	Determine that recorded transactions and related account balances are recorded in the proper accounts and all required disclosures are properly presented and clearly expressed so the financial statements are understandable.

Hidden in pre-lecture version

Example: Auditing notes payable

1. Obtain written confirmation from financial institutions regarding the amount of borrowings at year end. (Existence, Obligations, Valuation)
2. Obtain Copies of each loan agreement and:
   - Note the interest rate and interest payment dates. Determine that interest expense and interest payable are recorded in the proper amounts and in the proper period. (Valuation and Allocation, Cutoff)
   - Note the Principal payment dates. Determine that the current and noncurrent classifications are computed correctly. (Classification)
   - Note the existence of any restrictions placed on the company by this agreement. Determine whether the company is in compliance with all such restrictions. (Presentation)
3. Examine Canceled checks for any principal payments made during the period. (Valuation)
4. Review the minutes of the board of directors meetings to determine whether additional borrowing arrangements exist. (Completeness)
5. Inquire of management as to the existence of additional borrowing arrangements. (Completeness)

The audit process involves four steps:

- **Why, how, when,** and **who**
- Establish **scope** and **objectives** of the audit
- Identify risk:
  - **Inherent risk**: risk of control problems in absence of internal controls
  - **Control risk**: risk of material misstatement that will get through the internal control structure
  - **Detection risk**: risk that auditors and procedures will not detect material misstatement or error

Collection of evidence can be conducted in a several ways:

- **Observation**
- **Reviewing** documentation
- **Interviews**, discussions, and questionnaires
- **Physical examination** (e.g., inventory counts)
- Confirmation with **third parties**
- **Re-performing calculations** (e.g., estimates such as depreciation)
- Vouching supporting documents (e.g., **3 way matching**)
- **Analytical review** (examining trends and patterns)
- **Audit sampling**

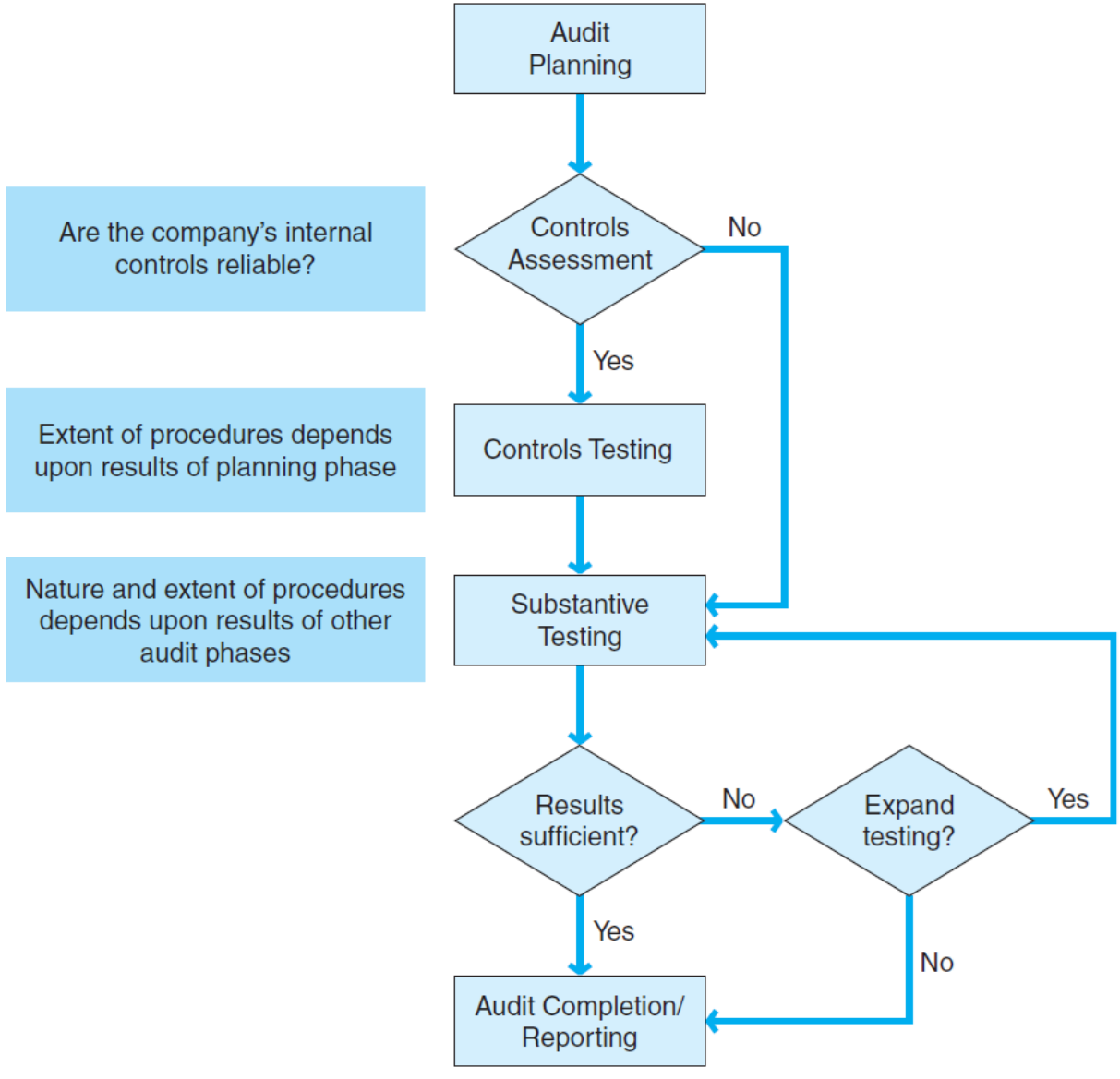
Evaluation of evidence involves the auditors conclusion that the evidence supports or does not support the assertion:

- Assess **quality** of internal controls
- Assess **reliability** of information
- Assess **operating performance**
- Consider need for **additional evidence**
- Consider **risk factors**
- Consider **materiality factors**
- Document **audit findings**

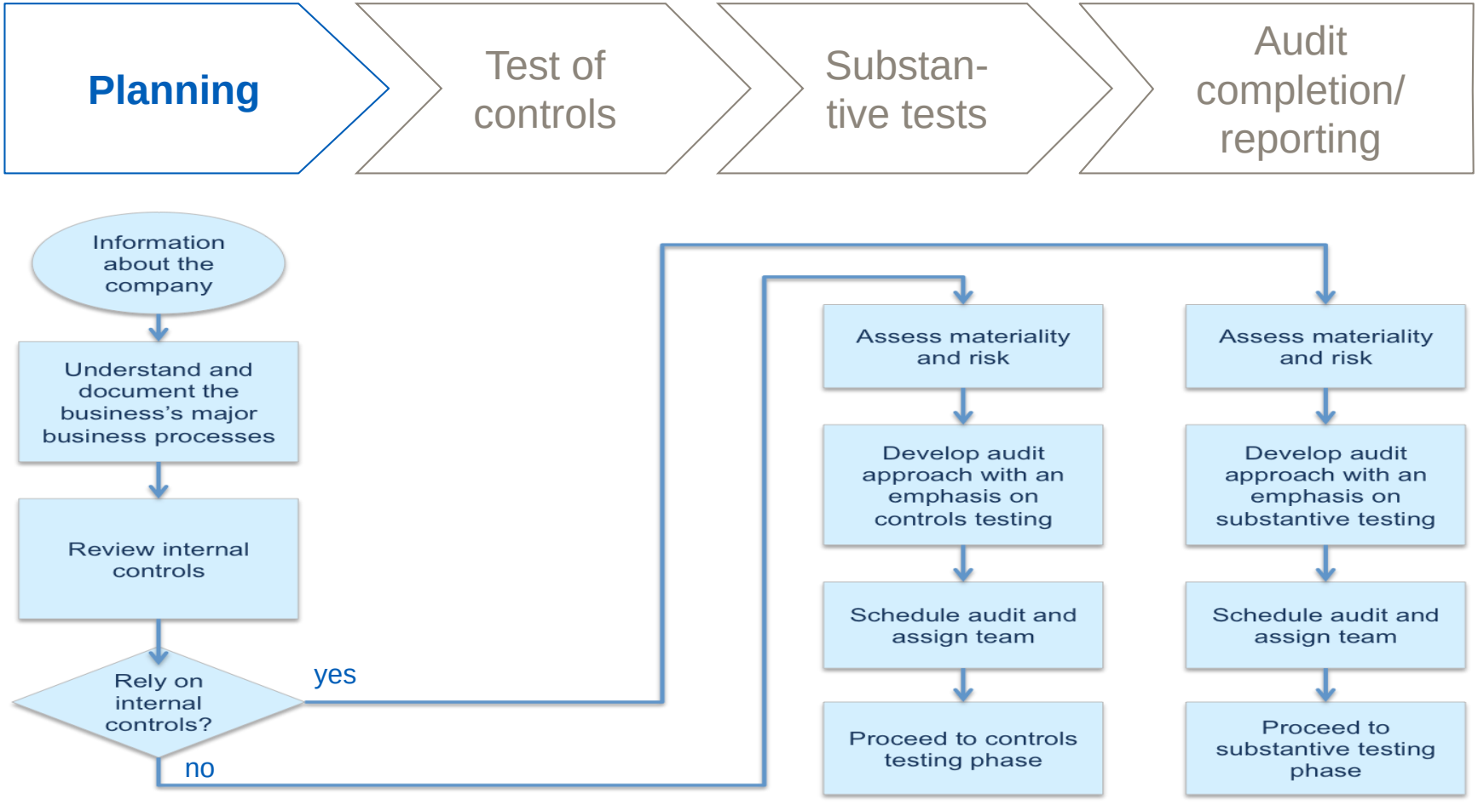
- **Communication** of results is in the form of a written report and often includes **recommendations** to management:
  - Formulate audit **conclusions**
  - Develop **recommendations** for management
  - Prepare **audit report**
  - **Present** audit results to management

III. AIS audits

AIS audit flowchart



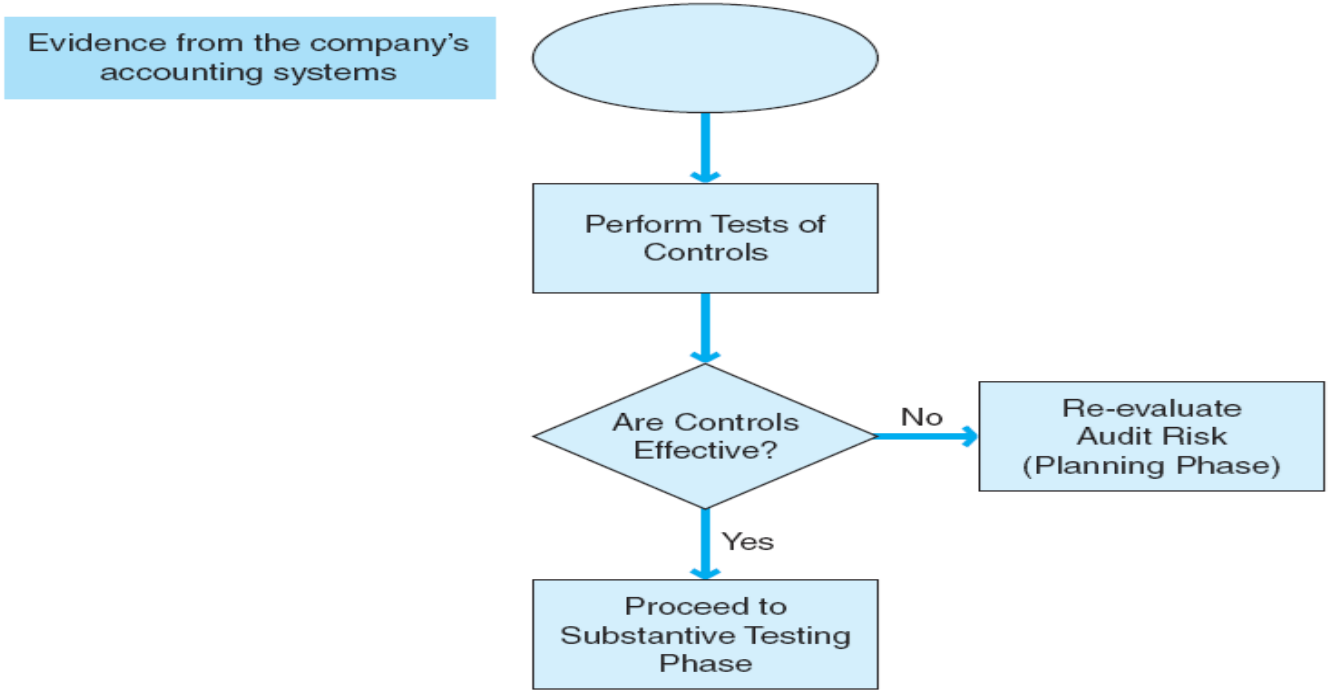
The AIS audit process involves four steps:



The **support** through **computers** can be classified into three levels:

- **Auditing around the computer**
- **Auditing through the computer**
- **Auditing with the computer**

  →Computer-assisted audit techniques (**CAAT**s)

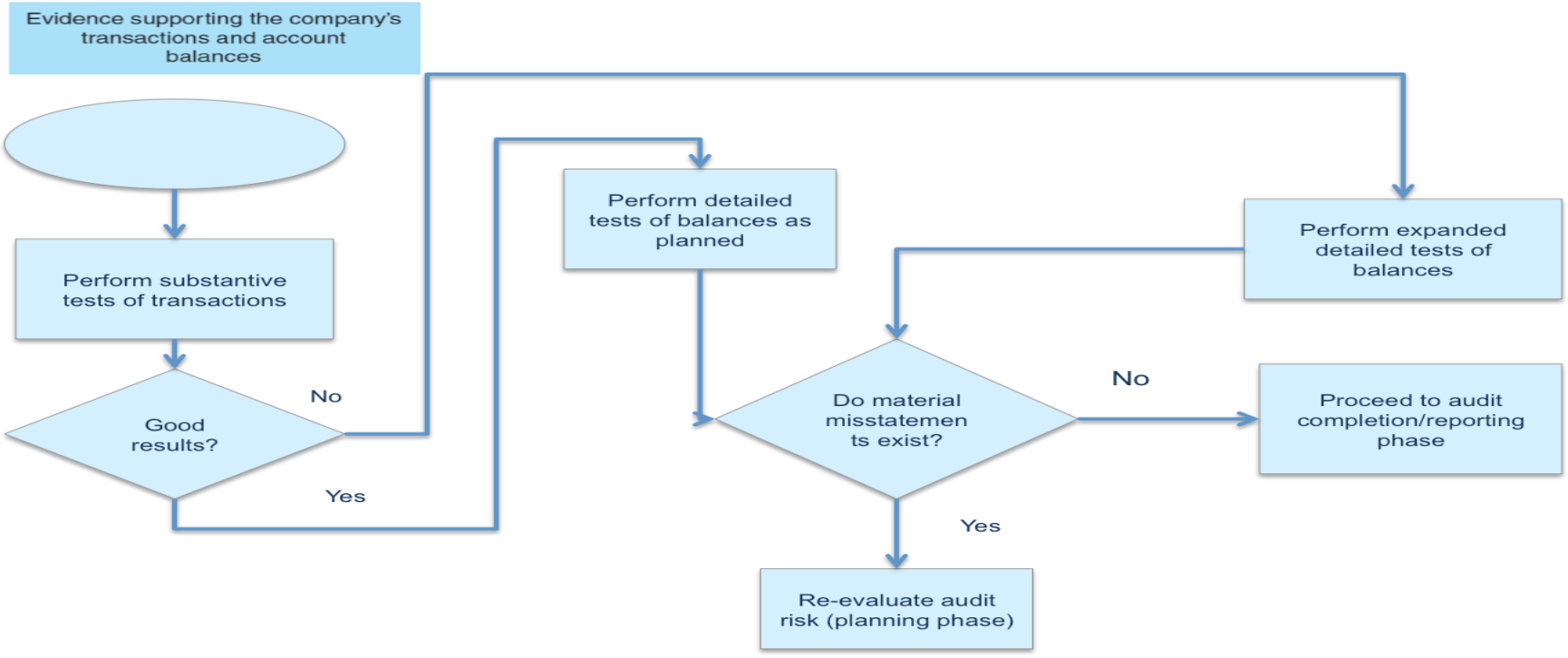


- **IT administration controls**: Audit tests include review for the existence and communication of company policies regarding:
  - **personal accountability** and segregation of incompatible responsibilities
  - **job descriptions** and **clear lines of authority**
  - **computer security** and **virus protection**
  - **IT systems documentation**

- **Security Controls:** To test external access controls, auditors may perform:
  - **Authenticity** tests.
  - **Penetration** tests
  - **Vulnerability** assessments
  - **Review access logs** to identify unauthorized users or failed access attempts

- **Application Controls:** Computerized application controls:
  - **Systems documentation**
  - **Main functions** of the computer applications
    - **Input controls** (e.g., Financial totals, Hash totals, Completeness or redundancy tests, Limit tests, Validation checks, Field checks)
    - **Processing controls** (e.g. Test data method, Program tracing, Integrated test facility, Parallel simulation, Embedded audit modules)
    - **Output controls** (e.g. reasonability tests, audit trail tests, rounding errors tests)

Planning | Test of controls | **Substan-tive tests** | Audit completion/ reporting



- **Substantive Testing** - tests of accuracy of monetary amounts of transactions and account balances
- **Computerized auditing tools** make it possible for more efficient audit tests such as:
  - mathematical and statistical calculations
  - data queries
  - identification of missing items in a sequence
  - stratification and comparison of data items
  - selection of items of interest from the data files
  - summarization of results into a useful format for decision making

Statistical analysis

- **Descriptives** can target further investigation
- Investigate **transaction dates** for suspicious activities (e.g. weekends, holidays, early mornings or late evenings)
- Search **duplicates** (company names, addresses, transactions,…)
- Sorting/indexing to identify **clusters**

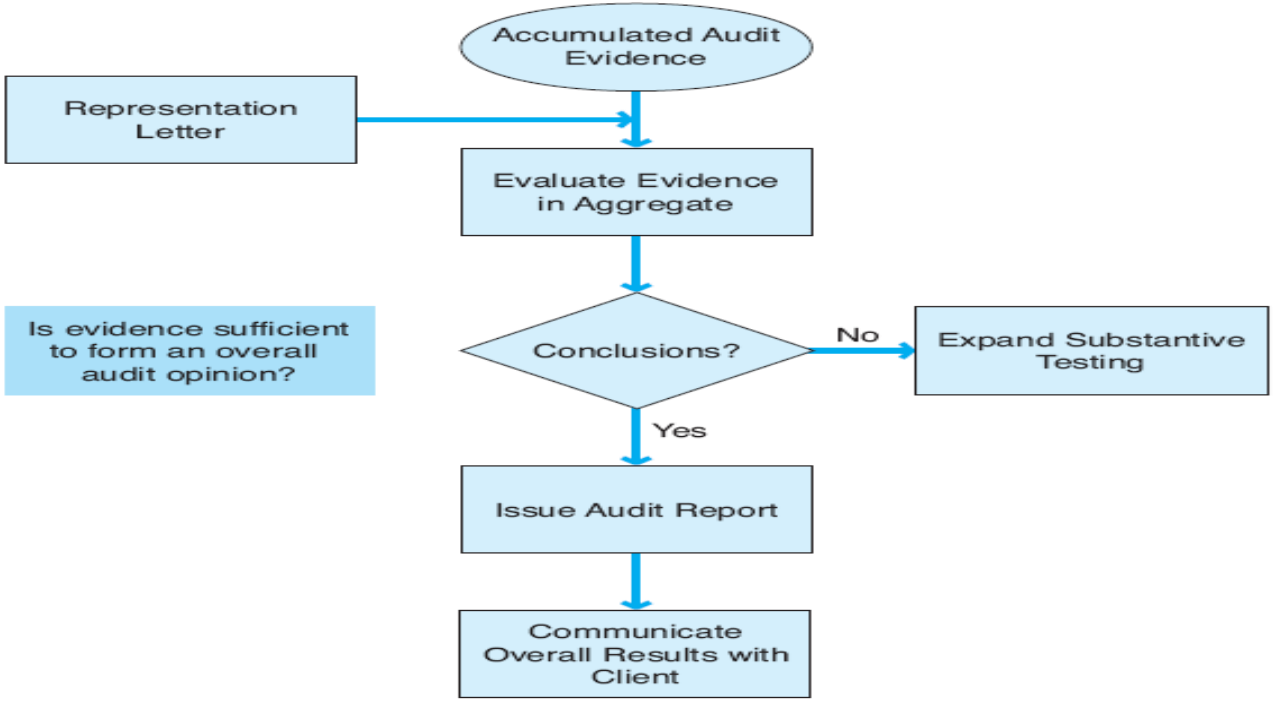
Who really are the champions of real-time fraud detection?
How?

- **Data mining can take two forms:**
  - Use of ‘intelligent’ software to continually monitor transactions for anomalous pattern recognition
  - Software to interrogate large data sets
- **Methodologies include:**
  - **Probability-based tools** (Neural networks, decision trees)
  - **Statistical tools** (link analysis, machine learning)

Non financial approaches to fraud detection

- Mine text for suspicious content
- Unstructured data can be accessed with
  - Dictionaries
  - Ontologies
- Make sure server permissions do not allow final deletion of mails

Planning → Test of controls → Substan-tive tests → **Audit completion/ reporting**



Four basic types of reports:

- Unqualified opinion
- Qualified opinion
- Adverse opinion
- Disclaimer

One more case…

IV. Special AIS Audit Issues

Some **audit techniques** used to **test controls** specifically in the use of PCs:

- Make sure that **PCs** and **removable hard drives** are **locked** in place to ensure physical security.
- Programs and data files should be **password protected**.
- Make sure **computer programmers** do **not** have **access** to systems operations.
- Software programs should **not permit** the users to make **program changes**.
- Ascertain that **computer-generated reports** are **regularly reviewed** by management.
- Determine the frequency of **backup procedures**.
- **Verify** the use of **antivirus software** and the frequency of virus scans.

- Using PCs, companies may use **IT environments** that involve:
  - networks,
  - database management systems,
  - e-commerce systems,
  - cloud computing, and/or
  - other forms of IT outsourcing.

What auditing issues might arise when a cloud is part of the audited system?

Concerns regarding the cloud:

- **Access** – data processed outside the enterprise bypasses internal controls!
- **Compliance** – Customer holds responsibility
- **Location** – No proof where data is actually stored
- **Data segregation** – needs to be encrypted, but loss risk
- **Recovery** – Backup plan?
- **Investigative support** – Impossible in cloud environme
- **Long-term viability** – data recovery guarantees

Hidden in pre-lecture version

- **Changes in a Client's IT Environment** - Auditors must consider whether additional audit testing is needed. Specific audit tests include verification of:
  - Assessment of user needs
  - Authorization for new projects and program changes
  - Adequate feasibility study and cost–benefit analysis
  - Proper design documentation
  - Proper user instructions
  - Adequate testing before system is put into use

Thank you!
Questions?