FOX | ITACS
Master of IT Auditing & Cyber-Security
Fox School of Business
TEMPLE UNIVERSITY

IT Audit Process

Prof. Liang Yao

Week Two – IT Audit Function

Why we need IT audit – A Case Study

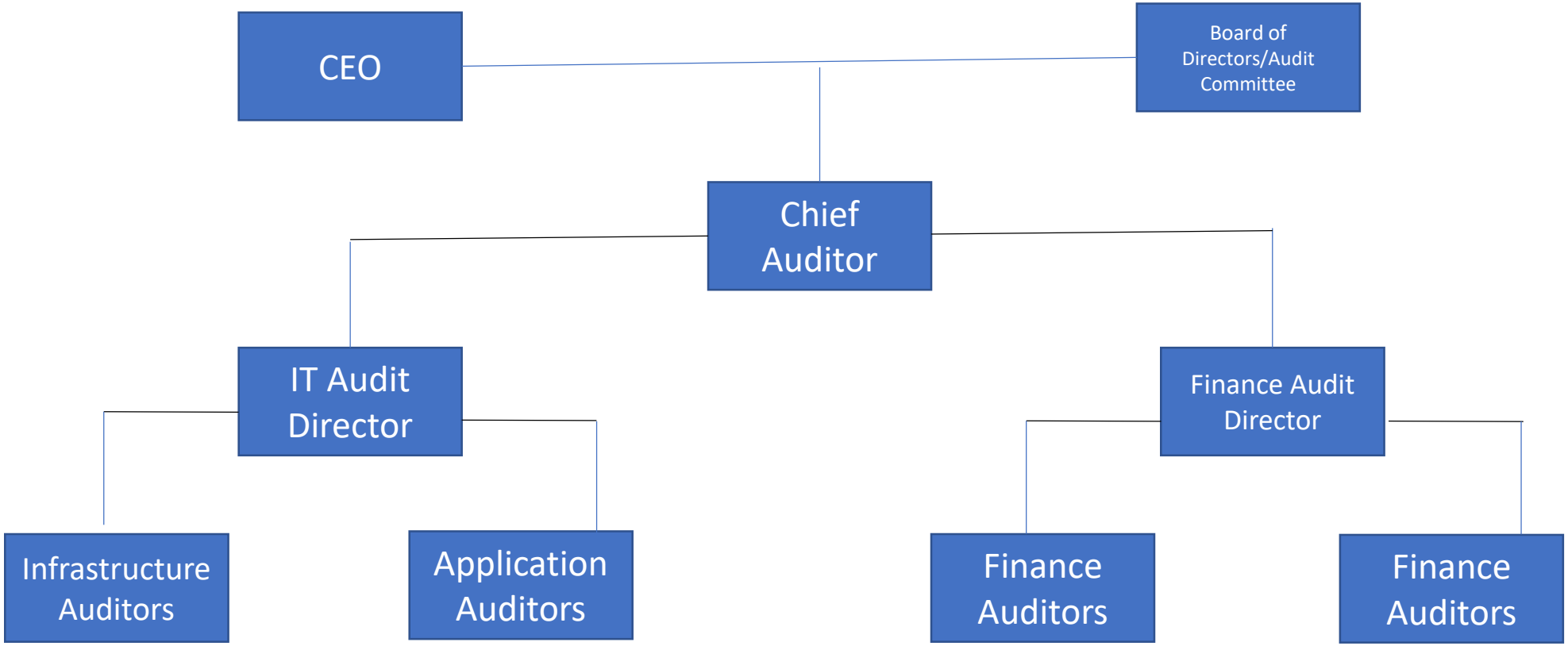
What You Can Learn about Risk Management from Societe Generale?

https://www.cio.com/article/2436790/security0/what-you-can-learn-about-risk-management-from-societe-generale.html

https://www.youtube.com/watch?v=WhiJjkSAJS0

- Inside threats
- Segregation of duties
- Monitoring system and escalation procedures
- Protecting credentials

A Sample IT Audit Org. Chart



IT Audit Engagements

- General Computer Audit
  - IT Strategy and planning
  - Information security
  - Change management
  - Software and hardware maintenance
  - Disaster Recovery, etc.
- Target IT Audit
  - Mainframe
  - Windows/Unix/Linux
  - Databases
  - Network
  - Cybersecurity

IT Audit Engagements (cont.)

- Application Audit
  - Electronic Funds Transfer (EFT)
  - Trading applications
  - Accounting applications
  - Enterprise Risk Management (ERP), etc.
- Integrated Audit
  - Work with other audit teams (financial, compliance, fraud, etc.)
- Pre-implementation review
  - SDLC
  - Cloud solution, etc.
- Continuous Monitoring

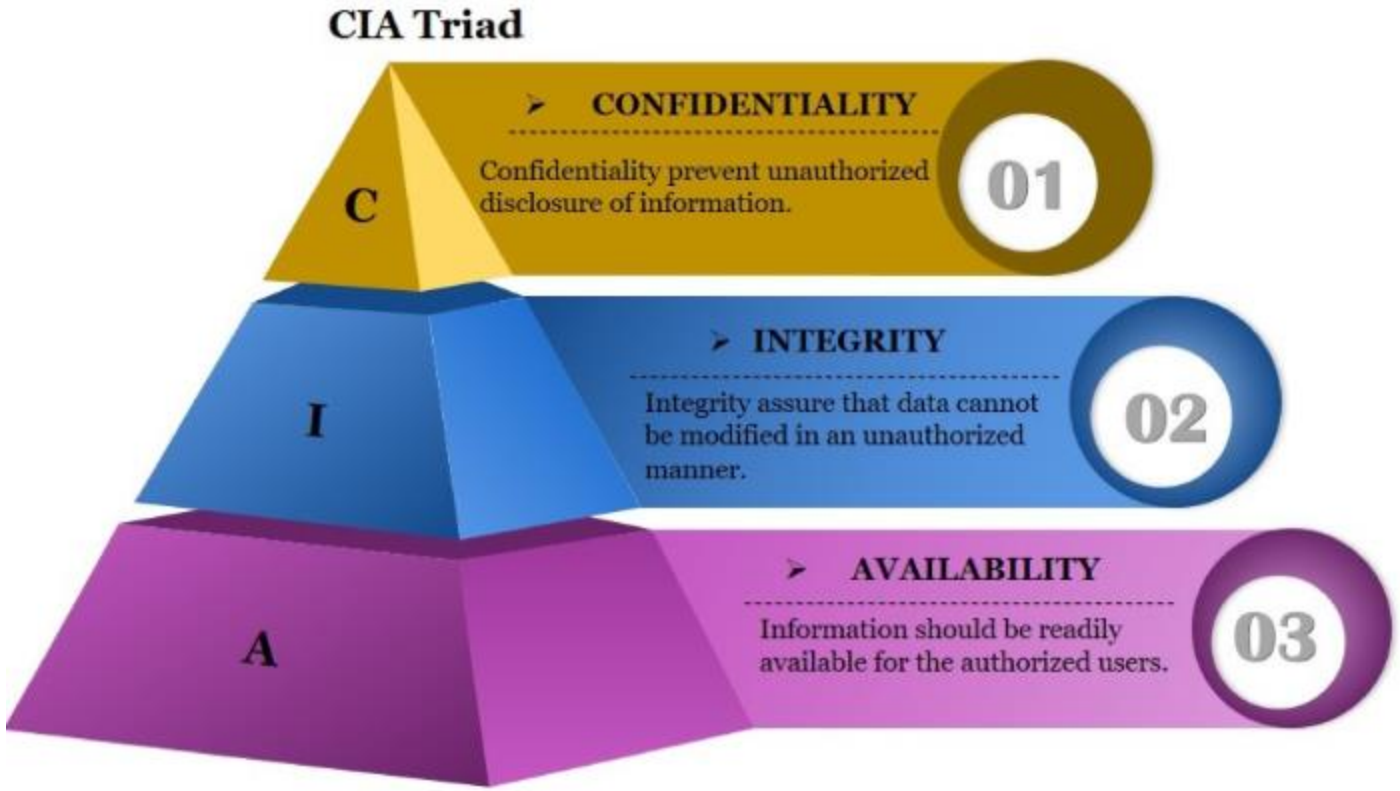
Audit Methodology Overview

- The need of an internal audit document to provide guidance of each audit phase (e.g. Audit Manual)
  - Following the *International Professional Practices Framework (IPPF)*
  - IT Audit – ITFA
  - Sample areas of coverage for methodology:
    - Risk assessment
    - Audit Planning
    - Fieldwork
    - Audit report
    - Issue Tracking, etc.

Audit Methodology Overview

- Audit subject (audit universe and entities)
- Audit objective
- Audit scope
- Preaudit planning
- Audit procedures and steps for data gathering
- Evaluating audit evidence and draw conclusion
- Communicating results to management
- Issuing report
- Tracking status of issue remediation

IT Audit and C.I.A Triad



ITAF – A Professional Practice Framework for IT Audit

- IS Audit and Assurance Standards
  - Mandatory
  - General Standards
  - Performance Standards
  - Reporting Standards
- IS Audit and Assurance Guidelines
- IS Audit and Assurance Tools and Techniques

ITAF – A Professional Practice Framework for IT Audit

- **General Standards**
  - 1001 Audit Charter
  - 1002 Organizational Independence
  - 1003 Professional Independence
  - 1004 Reasonable Expectation
  - 1005 Due Professional Care
  - 1006Proficiency
  - 1007Assertions
  - 1008Criteria

ITAF – A Professional Practice Framework for IT Audit

- **Performance Standards**
  - 1201 Engagement 1202 Risk Assessment in Planning
  - 1203 Performance and Supervision
  - 1204 Materiality
  - 1205 Evidence
  - 1206 Using the Work of Other Experts
  - 1207 Irregularity and Illegal Acts
- **Reporting Standards**
  - 1401 Reporting
  - 1402 Follow-up Activities

CISA Worldwide

More than 115,000 professionals have earned the CISA certification since it was established in 1978. The number of current CISAs by region is:

- Asia: 21,730
- Central/South America: 2,440
- Europe/Africa: 18,880
- North America: 33,640
- Oceania: 1,950

Source: https://www.isaca.org/About-ISACA/Press-room/Pages/ISACA-Certifications-by-Region.aspx

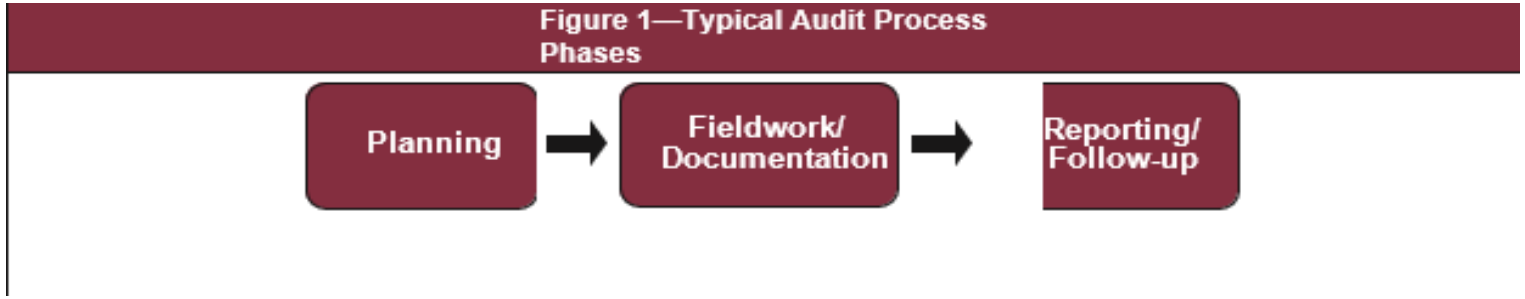
IT Audit responsibilities – Sample job description

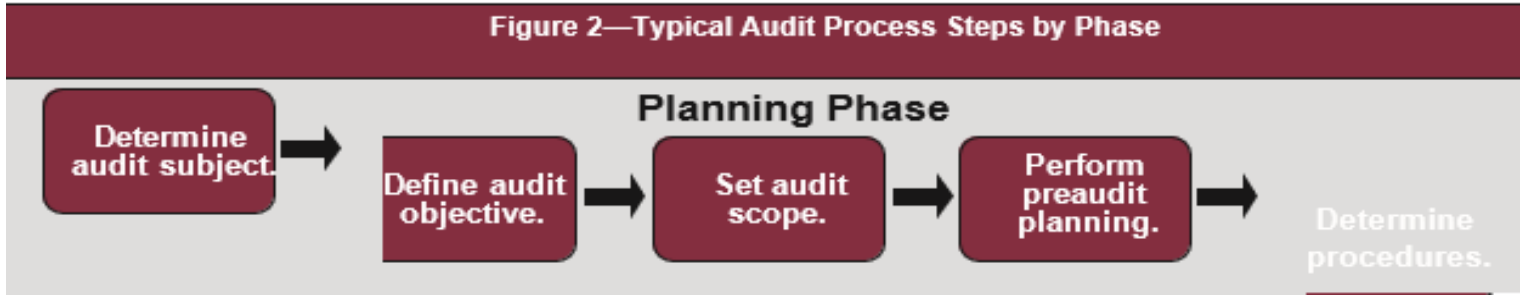
https://www.glassdoor.com/Job/it-audit-associate-jobs-SRCH_KO0,18.htm

IT Audit Proficiencies and Certifications

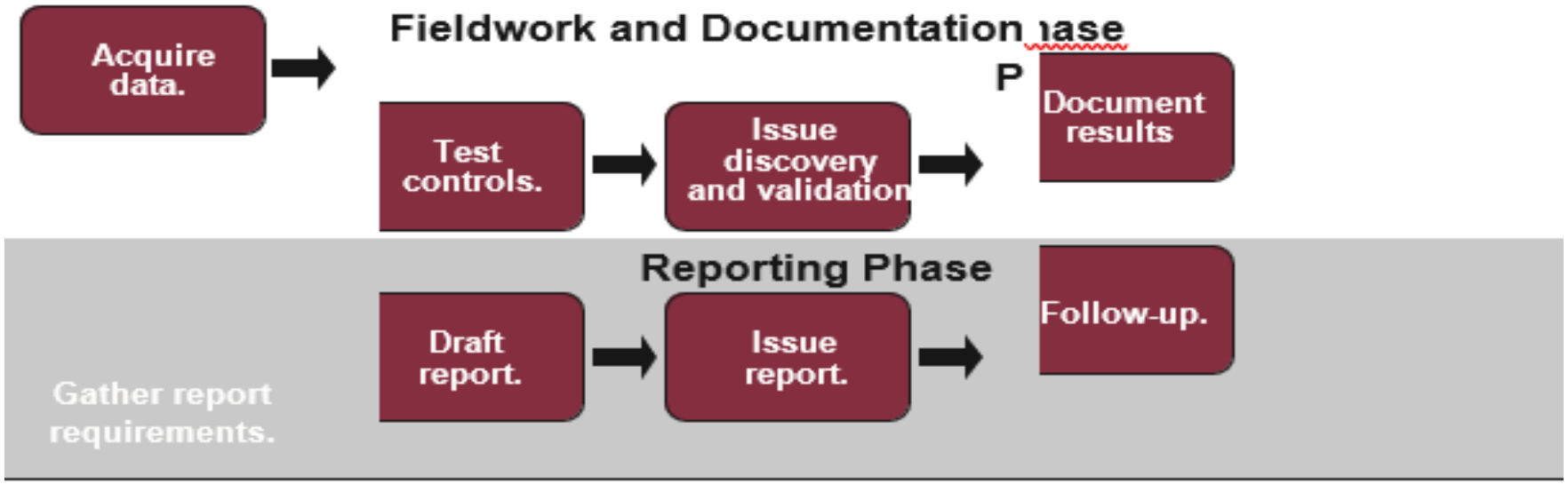
- Education background
- Professional job qualifications
- Relevant working experience
- Quality of work
- Certifications:
  - Certified Internal Auditor (CIA)
  - Certified Information System Auditor (CISA)
  - Certified Information System Security Professional (CISSP)
  - Six Sigma (PMP)
- Continuous Education

IT Audit Phases





IT Audit Phases (cont.)



Effect of Laws and Regulations on IS Audit (cont.)

- US Heal Insurance Portability and Accountability Act (HIPAA): HIPAA requires that the privacy of health records be protected, wherever they reside or whenever they are moved. That means the impact of HIPAA can be felt by nearly every aspect of IT operations, including messaging, storage, virtualization and even networking, so long as electronic PHI (ePHI) records are stored within or transferred over them. In turn, IT must be able to produce evidence of the security of these systems for compliance audits.
- US Sarbanes Sox (SOX): Internal Control Over Financial Reporting

Effect of Laws and Regulations on IS Audit

- The Gramm-Leach-Bliley Act (GLBA): also known as the Financial Modernization Act of 1999, is a federal law enacted in the United States to control the ways that financial institutions deal with the private information of individuals.
- FFIEC Regulations: https://ithandbook.ffiec.gov/
- PCI DSS: The Payment Card Industry Data Security Standard (PCI DSS) is a widely accepted set of policies and procedures intended to optimize the security of credit, debit and cash card transactions and protect cardholders against misuse of their personal information.

Ethic Matters

Arthur Anderson Case Study – Group Assignment #1

Research the failure of Arthur Anderson, one of the Big 5 public accounting firm with over 90 years history providing accounting and auditing services to its clients. Identify any ethic and due diligence related issues that leading to the firm's failure. What can we learn from Arthur Anderson's case.