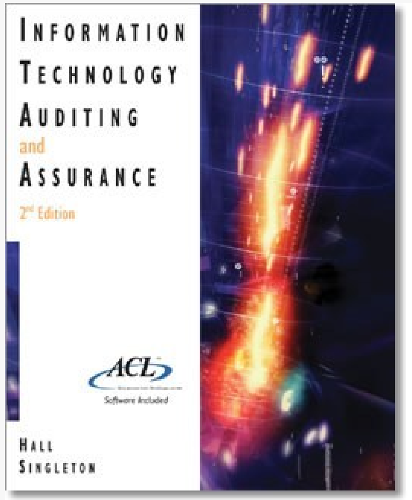
Lesson 2

Introduction to Auditing



ST2610

Security Policy & Incident Management

(SPIM)

Relationship between Audit & Policy

- Audit makes the policy meaningful and “alive”, by ensuring not only its compliance but also its efficiency and “compliability”
- In turn, the basis of reference of an audit is the policy

Auditing – Definition & Characteristics

- Auditing is a **systematic** process of **objectively** obtaining evaluation **evidence** regarding **assertions** about actions and events to **ascertain** the degree of correspondence between those assertions and establishing criteria and **communicating** the results to interested users.

Note the 6 Characteristics:

- Systematic
- Objective
- Evidence
- Assertions & Criteria
- Ascertain
- Communicate

- Auditing is a systematic, independent and documented process for obtaining audit

5 Primary Management Assertions

- 5 Primary Management Assertions, & Correlated Audit objectives & Procedures
    1. Existence or Occurrence
    2. Completeness
    3. Rights & Obligations
    4. Valuation or Allocation
    5. Presentation & Disclosure

Why Audit?

– Auditing is a management monitoring and evaluation technique providing feedback about the status of organisational processes important to the successes of a business or organisation

– Note: To maintain the value added to auditing, it must be carried out professionally, objectively and constructively

Why Audit?

(cont'd) ISO 27000

– To enable top management to obtain assurance and comfort that the company is in charge of and adequately handling its management responsibilities;

– To improve existing business processes and activities;

– To improve morale within the organisation;

– To solve problems or incidents within the organisation;

– To determine how effectively the organisation is achieving its stated business and quality objectives;

– To gather and analyse information upon which to make factual judgements;

– To identify where changes to business processes is required;

– To test the effectiveness and stability of the management system in achieving the stated business and quality objectives of the organisation

Why Audit?
(cont'd)

ISO 27000 (cont'd)

– Auditing is a management tool and a problem-solving process

– Note (again): To maintain the value added to auditing, it must be carried out professionally, objectively and constructively

– The auditor's function is to provide unbiased information to management for decision-making

– Audits must be carried out by staff with no direct responsibility in the area being audited

Audit – Ultimate Purpose

- For the betterment of quality of business, organisation, processes and assets (including data)
  - Productivity
  - Efficiency
  - Integrity of processes, services, assets
    - Ensuring the credibility of the organisation, services, systems and information
  - Feedback for improvement or finding and fixing any policy, service or asset
  - Risk Management and Mitigation
  - Due Diligence
  - Business Forward Planning, Interim Status Report

An Auditor is a Watchdog, Not a Bloodhound

- Auditors do not normally play policemen, investigate or look for crime, fraud or trouble
- Auditors are more like referees or qualified observers

AN AUDITOR IS A WATCHDOG, NOT A BLOODHOUND

THOMAS KOSHY

AUDITORS and company directors would benefit from reviewing two recent decisions rendered by the highest court in the land.

Last month, the Court of Appeal delivered comprehensive written judgments varying the outcome in the two distinct High Court claims against auditors, which were discussed in my article, "Whistling to the tune of $" (Jan 9).

In the Gaelic Inns case, the auditors failed to detect that over half a million dollars had been siphoned off by the company's finance manager. In the JSI Shipping case, the auditors failed to detect that one of the directors had drawn remuneration exceeding his entitlement by over half a million dollars.

The Court of Appeal affirmed the High Court decision that the auditors of Gaelic Inns had been negligent. But in the JSI Shipping case, the Court of Appeal reversed the High Court decision, holding that the auditors had been negligent there as well.

newscomment

It was not all bad news for the auditors though.

In both cases, the Court of Appeal also ruled that lapses in management on the parts of Gaelic Inns and JSI Shipping respectively had allowed the frauds to escape unnoticed. Accordingly, the auditors would only bear half the blame for the losses suffered by the firms.

While the two cases do not appear to have heralded any new developments in the law, the clear analysis is a boon to those who seek to better understand the liabilities of auditors and company directors.

To start with, the general principle remains: "If the auditor has genuinely exercised reasonable care in verification and still fails to detect a fraud ... liability would not invariably attach, for the detection and prevention of fraud *per se* is not typically within the scope of an auditor's duty."

So the issue of liability turns on whether the auditor has exercised reasonable care.

A key feature in both cases was that the auditors were actually aware of certain red flags in each of those cases but had failed to adequately investigate them.

In the Gaelic Inns case the failure by the finance manager to bank in hundreds of thousands of dollars in revenue showed up as gaps between the sales figures and the sums banked in. The auditors noticed the gaps and sought confirmation that the money was later banked in. But even when no confirmation was received, the auditors cleared the accounts.

Similarly, in the JSI Shipping case, the auditors had asked for written confirmation of the remuneration that the errant director was entitled to but later cleared the accounts without receiving such written confirmation.

So it is not difficult to appreciate why the auditors were held liable – they had failed to ensure that satisfactory answers were provided to questions they themselves had raised.

One interesting aspect of the JSI Shipping case is that the fraudulent director apparently allowed his excessive drawing of remuneration to be reflected openly in the accounts. The auditors argued that as there was no attempt at obfuscation or concealment, there was little cause for them to be suspicious.

But the Court noted that "his full disclosure could have reflected his bravado and/or confidence that his malfeasance would not be discovered, or it may just as well have been a tactical manoeuvre to mislead any investigative efforts". So, auditors should maintain their professional scepticism even when there is no surreptitious conduct.

It also bears noting that the Court of Appeal rejected arguments that detecting fraud was outside the scope of routine statutory audits done for a relatively low fee.

But it is the parts of the judgments relating to the lapses in management by the company directors that are more interesting.

It is not unusual, when a firm falls victim to fraud, for the auditors and the company's management to point fingers at each other. In both the cases, the Court of Appeal decided that the management had to share the blame with the auditors.

The Court acknowledged difficulty in deciding how much blame must rest with the auditors and management respectively, stating that such apportionment "must necessarily be done with a broad brush".

Unsurprisingly, in the final analysis, the blame was split down the middle in both cases. This establishes firmly that the courts will not hold the auditors fully liable if there have also been lapses in the management of the company.

No credence was given to the argument that the management could not be blamed as the auditors served as a check on management, and were therefore liable for any management lapses they failed to detect.

Building on the well-known characterisation of an auditor as "a watchdog, but not a bloodhound", it was stated: "Just because there is a watchdog on the premises, it does not follow that the occupants can safely forget to bolt the doors and omit to switch on the burglar alarm."

The Court noted "the dual responsibility imposed on auditors and directors to scrupulously adhere to the standard of car in the fulfilment of their occasionally over lapping duties", adding that "effective co porate governance requires both sets of pro fessionals to assiduously discharge thei responsibilities".

Another key point arose in the Gaeli Inns case. The directors had tried to argu that they could not be held accountable fo duties which they had already delegated t the fraudulent finance manager Ang.

The Court of Appeal disagreed, addin that "they cannot claim that they were ent tled to wholly rely on Ang to ensure that th accounts were in order. The fact that they ma have lacked accounting expertise did no completely exonerate them from their dutie to reasonably ensure that the respondent accounts were in order".

So, directors should not delude them selves that delegating responsibilities t other officers relieves them of their dutie And the same rules apply to non-executiv directors.

To enhance the reliability of corporate i formation, it is necessary that both auditors a company directors play their part. And whe they fail to do so, it should be expected th consequences will follow. As noted by th Court: "Market confidence that errant pr fessionals can be brought to book is an i portant feature of a mature financial centre

The writer is a legal academic who also trained briefly as an auditor. These are his personal views.

What's your view? Email us at news@newstoday.com.sg

2 Types of Audit

- Internal Audit
  - Independent appraisal function established within an organisation to examine and evaluate its activities as a service to the organisation
    - e.g.
      - Financial Audits
      - Operational Audits
      - Fraud Audits
      - IT Audits
      - Compliance Audits
- External Audit
  - Objective is that in all material respects, statements are a fair representation of the organisation
    - e.g. Compliance with
      - SGX requirements (for Singapore Public-Listed Companies)
      - IRAS & ACRA requirements (for Singapore Pte. Ltd. Companies)
      - IRAS & ROS requirements (for Singapore Registered Societies)
      - Sarbanes Oxley Act (for US Companies)
      - Industry Regulations
- e.g.
  - MAS' TRM for Financial Institutions
  - Cybersecurity Code of

Generally Accepted Auditing Standards

- General Standards
  - The auditor must have adequate technical training and proficiency.
  - The auditor must have independence of mental attitude.
  - The auditor must exercise due professional care in the performance of the audit and the preparation of the report.
- Standards of Field Work
  - Audit work must be adequately planned.
  - The auditor must gain a sufficient understanding of the internal control structure.
  - The auditor must obtain sufficient and competent evidence.
- Reporting Standards
  - The auditor must state in the report where statements were prepared in accordance with generally accepted principles.
  - The report must identify those circumstances in which generally accepted principles were not applied.
  - The report must identify any items that do not have adequate informative disclosures.
  - The report shall contain an expression of the auditor’s opinion on the statements as a whole.

IT Audit

- Provide audit services where processes or data, or both, are embedded in technologies
  - Subject to ethics, standards and guidelines
  - Scope of IT audit coverage is increasing
  - IT governance is becoming part of corporate governance

"…. most accounting transactions to be in electronic form without any paper documentation because electronic storage is more efficient.
… These technologies greatly change the nature of audits, which have so long relied on paper documents."

2 Types of IT Audit

- General
  - To ensure proper and efficient use of IT resources in line with business objectives
    - No wastage or misuse
    - e.g. For baseline for technology refresh, system update or capacity planning
- Security
  - To ensure IT has adequate and proper safeguards, practices and policies to minimise risks
    - Protection of assets, data, systems and services

Internal v. External Audit

- Internal Audit
  - Done by one or more staff members of the organisation
  - Internal audit team imposes independence on self
  - Broad scope of audit
    - e.g. Financial matters, Operational matters, Capacity Planning, Technology or Process Refresh Review
  - Represent interest of the organisation
  - May be a preparation for external audit
- External Audit
  - Done by independent professional auditors
  - Independence defined by government, standard or industry
  - Required by government for public-listed companies, and large private companies above a certain annual revenue level
  - Represents interest of outsiders i.e. “the public”
  - Standards, guidelines, certifications governed by national and/or industry authorities

Audit – Corollary & Operational Objectives

- Establish Accountability
- Establish Ownership, Chain of Command, Chain of Communication, Chain of Escalation
- Ensure Consistency of Processes, Policies and Behaviour
- Ensure Adequate Policies are In Place and are Working Properly
- Ensure Operational Integrity and Consistency, and Proper Treatment of Assets (including data)
- Ensure Morale of Stakeholders (shareholders, managers, staff, business partners, suppliers, customers and clients, and the public)
- Meet Compliance

– Whilst meeting the ultimate purpose of audits

i.e. For the betterment of quality of business, organisation, processes and

Audit Programme Objectives

ISO 27000

- Top management should ensure that the audit programme objectives are established to direct the planning and conduct of audits and should ensure the audit programme is implemented effectively.
- Audit programme objectives should be consistent with and support management system policy and objectives.
- e.g.
  - To contribute to the improvement of a management system and its performance
  - To fulfil external requirements e.g. certification to management system standard
  - To verify conformity with contractual requirements
  - To obtain and maintain confidence in the capability of a supplier
  - To determine the effectiveness of the management system
  - To evaluate the compatibility and alignment of the management system objectives with the management
  - System policy and the overall organisational objectives

Audit Programme Components

- Objective
- Scope
  - Incumbent Policy Documents and any other relevant documents
  - Previous Audit Reports
  - Statement of Applicability
  - Exceptions
  - Standards
  - Sampling (if any)
- Plan
- Logistics
  - Meeting dates, time, with whom
  - Facilities e.g. Meeting Room, Audit Room, Document, Support Services, Tools Required, Client Contract Officers, Client Accompanying Officers
- Timing
  - Start Date, End Date, Expected Duration, Milestones, Interim Meetings
  - Visit to different sites (Expected Date, Time, Duration)
  - Draft Final Report Meeting
  - Interim & Final Reports and Presentation (if any) Expected Dates

Audit Programme |

Phases

1. Planning
   - Understanding Client’s Internal Control
2. Obtaining Evidence
   - Tests of Controls
   - Tests of Evidence (Reports, Records, Processes)
   - Substantive (Additional) Testing e.g. Using Computer Aided Tools, Analytical Procedures, etc.
3. Ascertaining Reliability
   - Materiality
4. Communicating Results
   - Audit Opinion i.e. Reporting

Audit Programme Planning

- Process of determining in advance what to do, when and how to do it, and by whom
- Development of overall strategy
- Optimises transfer of knowledge from one audit exercise to another
- Must be written and documented for approval

- Purpose & Advantage
  - Adequate attention given to important areas of audit
  - Identify potential problems
  - Audit completed expeditiously and timely
  - Utilise staff properly
  - Determine audit procedures to use

“If you fail to plan, you are planning to fail.”

Audit Programme Planning
(cont'd)

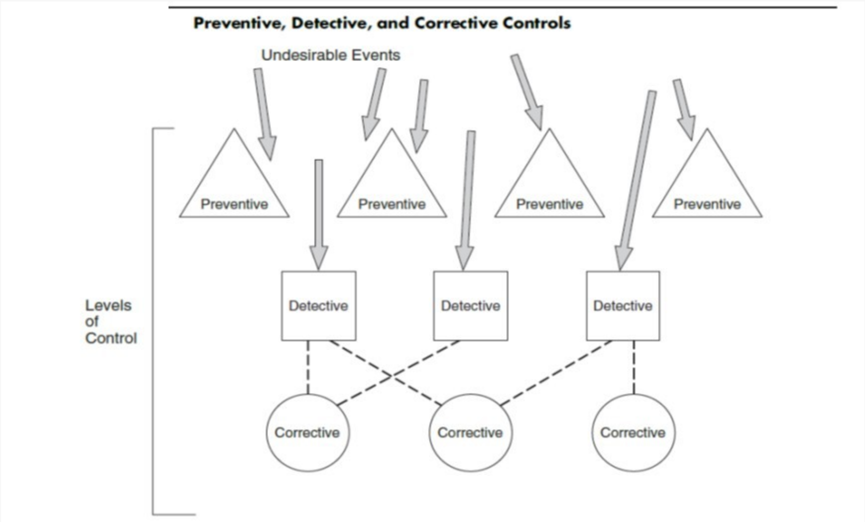
- Audit Objectives
  - Central objective which an audit is to accomplish
- Audit Scope
  - Area to be covered
  - Basis to conduct audit
  - Acts as defence for auditor in case of misunderstanding or allegation of areas not covered
- Elements
  - Understanding auditee's organisation
  - Determining audit objectives and scope
  - Performing risk analysis
  - Conducting an internal control review
  - Setting the audit scope and objective
  - Developing audit approach or audit strategy

Audit Risks

- Audit Risk * EXTREME CASE
  - The probability that the auditor will give an inappropriate opinion on the statements
    - i.e. the statements will contain materials misstatement(s)
      - i.e. The audit exercise is flawed or failed
- Control Risk
  - The probability that the internal controls will fail to detect material misstatements
    - Control itself is flawed in the first place, thus compromising the audit
- Detection Risk
  - The probability that the audit procedures will fail to detect material misstatements
- Inherent Risk * EXTREME CASE
  - Risks that cannot be controlled
    - Material v. Immaterial
    - e.g. Economic conditions, weather, change of industrial trend, parent company M&A
    - Needs to be taken into account at audit planning stage to ensure minimal errors or misstatements

Controls

- Policies, Practices and Procedures designed to:
  - Safeguard assets
  - Ensure accuracy and reliability
  - Promote efficiency
  - Measure compliance with policies (both internal policies and external industrial and/or governmental regulations)
- Types of Controls
  - Preventive Controls
  - Detective Controls
  - Corrective Controls
  - Predictive Controls



Elements of an Control Environment

- Integrity and ethical values of the management
- Structure of the organisation
- Participation of the organisation’s board of directors & audit committee
- Management’s philosophy and operating style
- Procedures for delegating responsibility and authority
- Management’s methods for assessing performance
- External influences
- Organisation’s policies and practices

Techniques Used to Understand an Control Environment

- Understand the client's business and industry
- Describe the possible activities or tool for each control
- Study the organisation structure
- Determine if the board and audit committee are actively involved
- Assess the integrity of the organisation's management
- Conditions conducive to management fraud

The IT Environment

- There has always been a need for an effective internal control system
- Design and oversight of that system has typically been the responsibility of accountants
- The IT environment complicates the paper systems of the past
  - Concentration of data
  - Expanded access and linkages
  - Increase in malicious activities in system v. paper
  - Opportunity that can cause management fraud (i.e. override)

Controls |

Limitations

- Honest Errors
- Circumvention via Collusion
- Management Override
- Coping with Changing Conditions
  - e.g. Especially in companies with high growth

Risks of Weak Controls

- Intentional & Accidental
- Risks – Potential threat to compromise use or value of organisational assets
- Types of Risk
  - Theft of Assets
  - Modification of Assets
    - Including corruption of information and/or information systems
  - Destruction of Assets
  - Disruption of (IT) Systems and/or Services

Baring loses $1 billion due to lack of internal controls

On February 23, 1995, a 232 year-old British bank, Baring Bros. and Co., went bankrupt due to a loss of $1 billion in futures trading by an employee, Nick Leeson. A statement by the Singapore International Monetary Exchange (SIMEX) attributed the loss to a *failure of internal controls*. [Associated Press, March 5, 1995]. Senior executives conceded that controls should have been much tighter. The organization ignored several warning signs of internal control weaknesses over several years:

- In *March 1992*, a senior executive in Singapore wrote a letter to the head of the equity department in London stating, "My concern is that once again we are in danger of setting up a structure which will subsequently prove disastrous and with which we will succeed in losing either a lot of money or client goodwill or probably both. In my view, it is critical that we should keep clear reporting lines and if this office is involved in SIMEX at all then [Mr Lesson] should report to the Singapore office operations department not the London derivatives department."
- An internal audit report in the summer of 1994, cited lax internal controls and made a specific recommendation that the trading and settlement duties be separated. Mr Lesson at the time was in charge of both duties.
- Mr Lesson used an error account to hide trades that he did not want his superiors to know about.

Managers were reluctant to impose tight controls, which might have reduced profits and bonuses.

Source: Brauchli, Marcus W., Bray, Nicholas, and Sesit, Michael, "Barings PLC Officials May Have Been Aware of Trading Position," (1995) *Wall Street Journal*, March 6, 1995, p. 1, 6.

Risk Assessment

- Changes in Environment
- Changes in Personnel
- Changes in Information System
- New IT
- Significant or Rapid Growth
- New Products or Services (Experience)
- Organisational Restructuring
- Foreign Markets
- New Accounting Principles

Monitoring

- Separate procedures e.g. tests of controls
- Ongoing activities
  - Embedded Audit Modules (EAMs)
  - Continuous Online Auditing (COA)
- Use of management reports
- Summarising activities e.g. highlighting trends, identifying exceptions

Controls | 2 Important Frameworks

- Committee of Sponsoring Organisations (COSO)
- Sarbanes-Oxley Act (SOX)

COSO

- A **management perspective model** for internal controls
  - Developed over many no. of years
  - AICPA, AAA, FEI, IMA, IIA
- **Ultimate Objective** * IMPORTANT
  - **The best deterrent to fraud is strong internal controls**
- Widely Adopted
  - AICPA adopted it into auditing standards SAS No. 78 (Consideration of Internal Control in a Financial Statement Audit)

COSO | Internal Control Framework

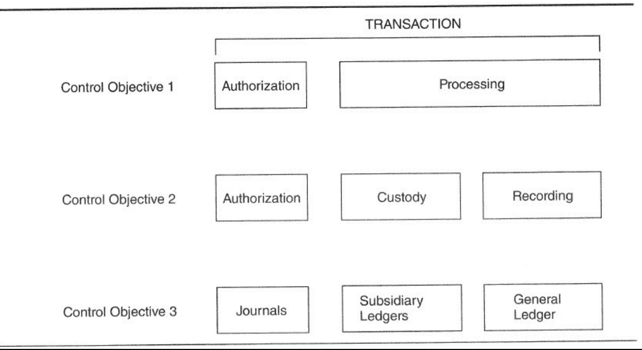
The COSO Cube

COSO | Control Activities

- Independent Verification
  - Management can assess
    - e.g. the performance of individuals, integrity of the data in the records
- Transactional Authorisation
  - e.g. Sales only to authorised customers, Sales only if available credit limit
- Segregation of Duties
  - Principle: Fraud requires collusion
  - The “Four Eyes Principles”
  - e.g. Separate various steps in process
  - e.g. Incompatible duties
    - Authorisation v. Processing (e.g. Sales v. Authenticate Customers)
    - Custody v. Recordkeeping (e.g. Custody of Inventory v. DP of Inventory)

FIGURE 1.5

Segregation of Duties Objectives



- Supervision
  - Serves as compensating control when lack of segregation of duties exists by necessity
- Accounting Records
- Access Controls
  - Direct (Assets)
  - Indirect (Documents that controls the assets)
  - Disaster Recovery

SOX

- §404 – Management Assessment of Internal Control
  - Management is responsible for establishing and maintaining internal control structure and procedures
  - Must certify by report on the effectiveness of internal control each year, with other annual reports
  - **Ultimate Objective**
    - **Top management is responsible for proper financial control, practice and reporting**
- §302 – Corporate Responsibility for Incident Reports
  - Financial executives must disclose deficiencies internal control and fraud (whether fraud is material or not)

SOX | SOX v. IT

SOX does not directly regulate Information Technology. However, IT is the backbone of the financial processes that the law regulates. Section 302 requires that the CEO, CFO and an attesting public accounting firm certify the accuracy of financial statements and must certify that statements fairly present the operations and financial condition of the issuer. It also requires that material information that is used to generate reports be retained and made available to the public. This **directly affects the IT and security** departments because it is primarily IT systems that generate these periodic reports and which control e-mail, the main method of communication within most organizations. These systems must remain secure and reliable.

Section 404 is the most pertinent section within Sarbanes-Oxley to issues surrounding information security. It addresses the necessity of corporate management to be fully accountable for the integrity of all data associated with their financials. It states that management teams of public companies must establish and maintain adequate "Internal Controls" over their financial reporting systems to safeguard against unauthorized and improper use of financial information. Internal Controls are defined as "all control methods a company uses to prevent, detect and correct errors and frauds that might get into financial statements".

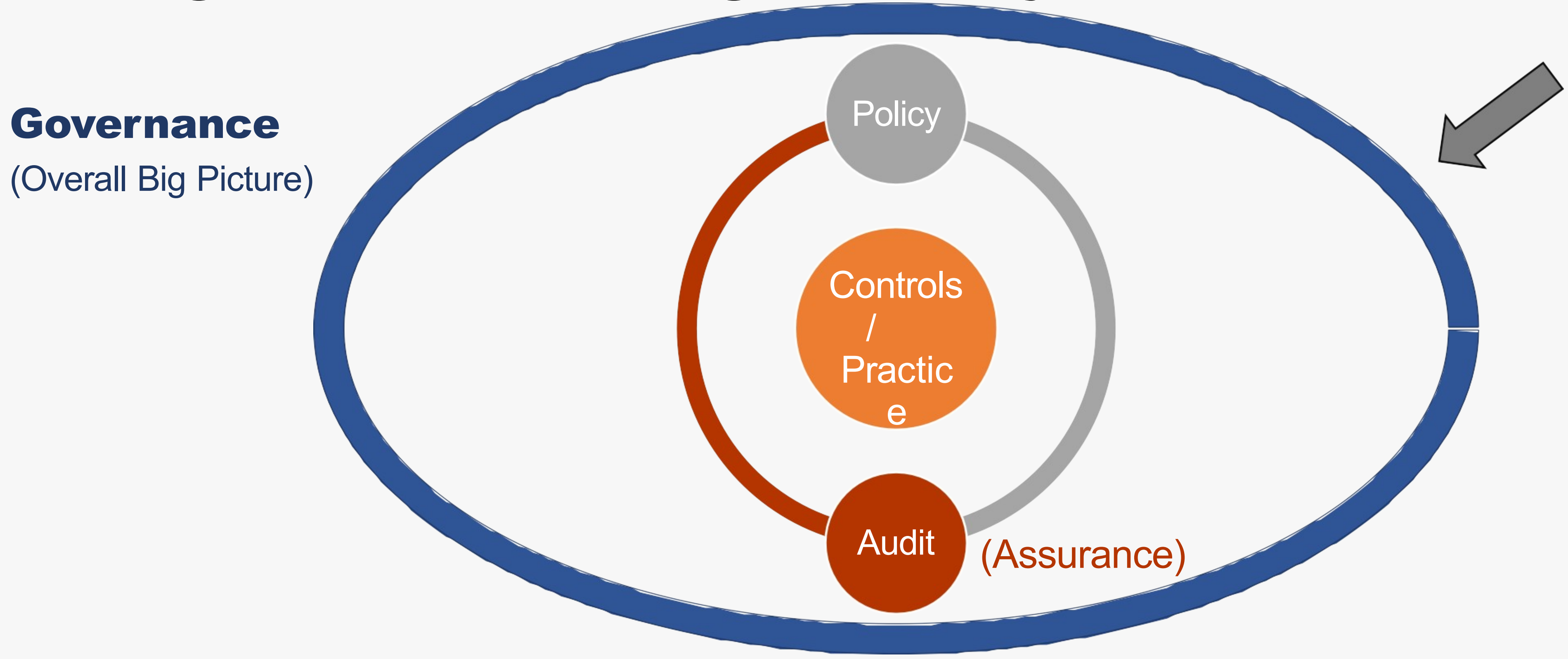
– SOX is not an IT law. But because of the great dependence of IT today in financial systems and services – regarding data, transactions, calculations, analysis, storage, communications, reporting etc. –, in order to meet SOX requirements, indirectly, the organisation's IT and security controls need to be adequate and in good order.

SOX | The Significance

- The 1st law that holds top management responsible for the firm's operating integrity
- The 1st law where top management go to jail for serious non-compliance
  - Chairman, CEO, CFO, COO, MD, ED, etc.
  - Greatly increases compliance rate
  - Greatly improve IT and security
- Other countries outside the US – including Singapore – start to adopt parts, ideas or shades of it

Audit – Pinnacle of IT Governance

- Responsibility of executives and board of directors.
- Consist of the **leadership**, **orgainsational structures** and **processes** that ensure that the enterprise's IT sustains and extends the **organisation's strategies** and **objectives**.



Forces Driving Governance

- Business & IT Alignment Return-of-Investment (ROI)
- Project Execution
- Security
- Compliance

Governance Needs a Management Framework

– Driving Forces of Governance Domains

ISO/IEC 27001:2013 Information security management systems

ISO 27000 family of standards:

ISO/IEC 27001 –specifies the requirements for an ISMS
ISO/IEC 27002 –guideline for the implementation of the controls in Ar

ISO/IEC 27000 – a general overview of information security and terms and definitions
ISO/IEC 27003 –general guidance for the implementation of an ISMS
ISO/IEC 27004 –advice on how organizations can monitor and measure the performance of their ISMS
ISO/IEC 27005 –guidance on risk management and ISO/IEC 27006 –for audit
and certification of ISMS ISO/IEC 27007 - guideline on how to audit an ISMS
-sector specific -
ISO/IEC 27011 –application of security controls in telecommunication
ISO/IEC TR 27015 –information security management in financial services

… and others