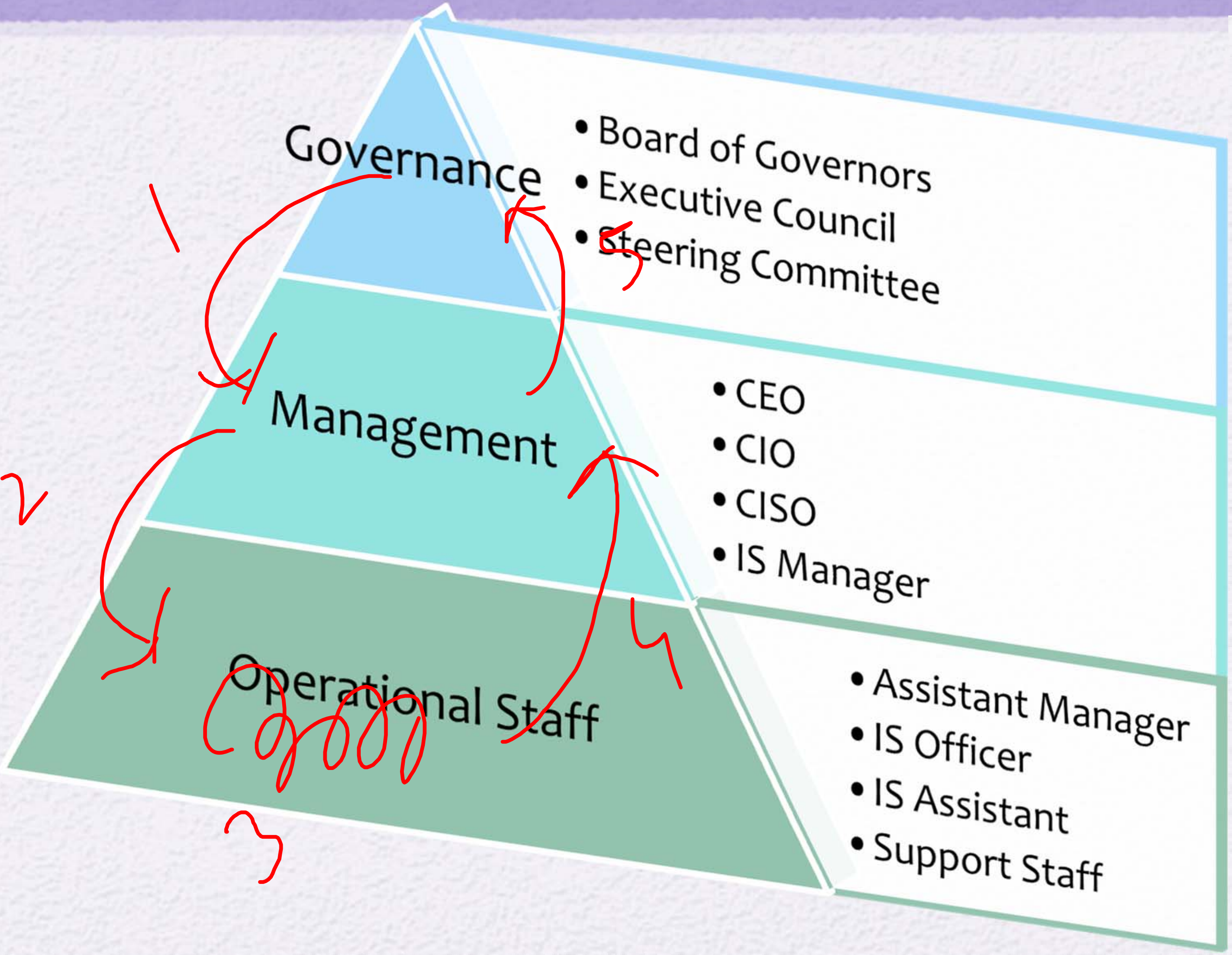
Organizational Hierarchy - Roles



Governance

- Board of Governors
- Executive Council
- Steering Committee

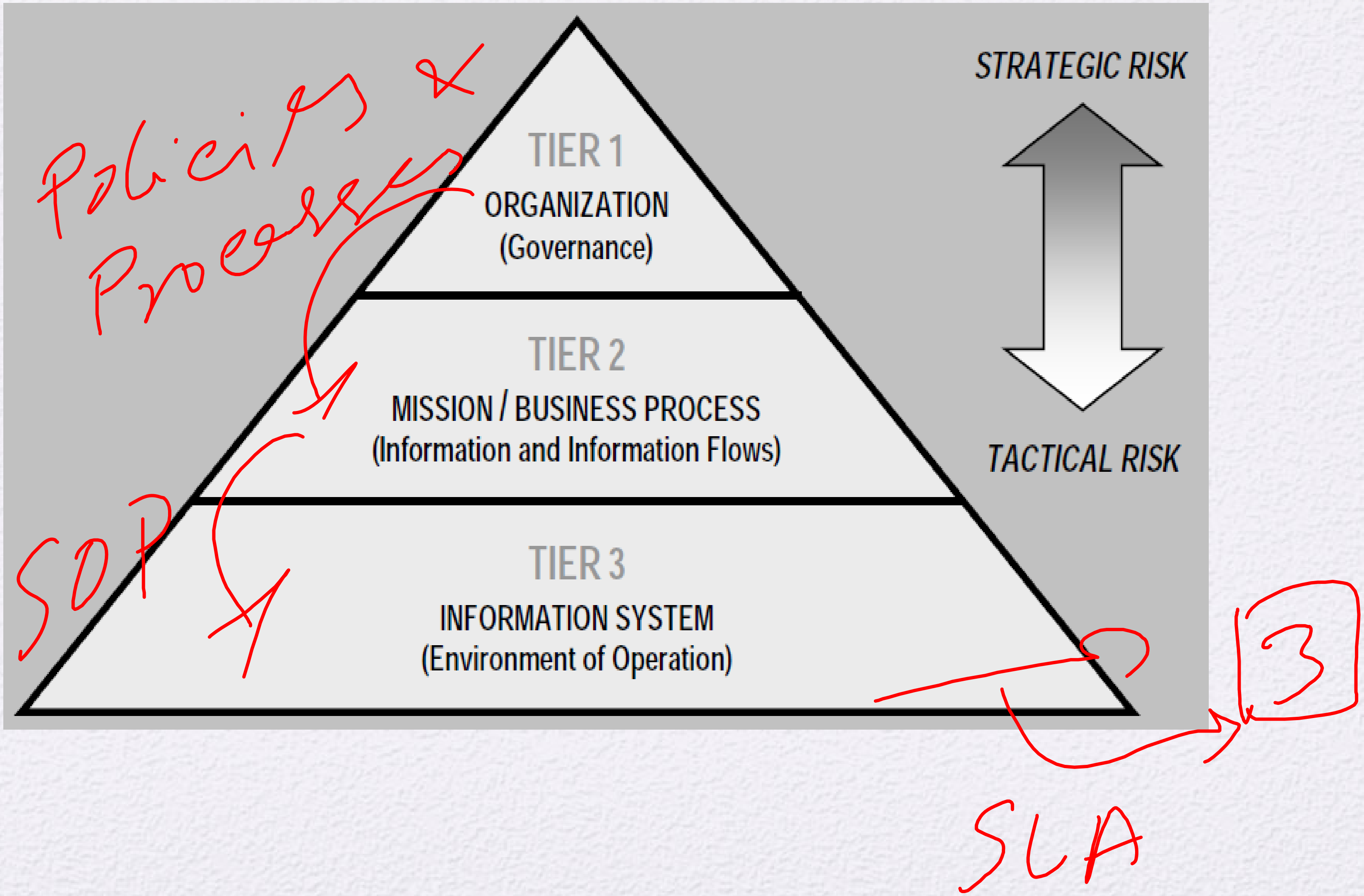
Management

- CEO
- CIO
- CISO
- IS Manager

Operational Staff

- Assistant Manager
- IS Officer
- IS Assistant
- Support Staff

Multi-Tiered Risk Management



TIER 1

ORGANIZATION
(Governance)

TIER 2

MISSION / BUSINESS PROCESS
(Information and Information Flows)

TIER 3

INFORMATION SYSTEM
(Environment of Operation)

STRATEGIC RISK

TACTICAL RISK

Policies &
Processes

SOP

3

SLA

IT Governance

- IT Governance is not IT management.
  - IT governance is an extension of Corporate Governance
  - It originates from the Board of Directors.

- As an extension of corporate governance, IT governance is a **top-down** model, never bottom-up.

ISACA Definition of IT Governance

- ISACA = Information Systems Audit and Control Association
  - www.isaca.org

- The responsibility of executives and the board of directors is to provide:
  - **Leadership**
  - **Organizational Structures**
  - **Processes**

IS Governance

- Security Governance is the collection of practices related to defining, directing, and supporting the security efforts of an organization.

- Information security governance provides the mechanisms:
  - for the board of directors and management
  - to have the **proper oversight to manage the risk** to the enterprise
  - to an acceptable level.

Security Plans

- **Strategic Plan**
  - Longer term plans (3 to 5 years)
  - Establishing security policies and processes aligned with the business goals and mission
- **Tactical Plan**
  - Shorter term plans (6 months to 1 year)
  - Initiate, implement, and deploy specific projects to achieve the goals
- **Operational Plan**
  - Set team objectives, assist and monitor staff with work progress
  - Implement procedures to maximize operating efficiency

Question ?

- Tactical security plans are BEST used to:
  A. Establish high-level security policies
  B. Enable enterprise/entity-wide security management
  C. Reduce downtime
  D. Deploy new security technology

- Answer: D
  - Tactical plans provide the initiatives to support and achieve the goals specified in the strategic plan.
  - These initiatives may include deployments such as establishing an electronic policy development and distribution process, implementing robust change control for the server environment, reducing vulnerabilities residing on the servers using vulnerability management, implementing a disaster recovery program, or implementing an identity management solution.
  - These plans are more specific and may consist of multiple projects to complete the effort.
  - Tactical plans are shorter in length, such as 6 to 18 months to achieve a specific security goal of the company.

Security Policy

- Policies should survive two or three years
  - These should be reviewed and approved at least annually.
- Technical implementation details are not included in a policy.
- Policies must be written technology independent.
- Technology controls may change over time as an organization’s risk profile changes and new vulnerabilities are found.

Security by Design

- Security is much less expensive when it is built into the application design versus added as an afterthought at or after implementation.

Security Roles

- Establishing clear, unambiguous security roles has many benefits to the organization such as:
  - Defined responsibilities to be performed,
  - Defined roles to perform the tasks,
  - Establishes personal accountability,
  - Reduces departmental turf battles,
  - Establishes continuous improvement.

→ dedicated ✓

→ Shared ✗

Ownership roles

- **Mission or Business Owner**
  - Establishes organizational mission and business processes
  - Balances between security controls & business requirements
  - Provides input to the risk management strategy
- **System Owner**
  - Responsible for system lifecycle activities and compliance requirements
  - In coordination with Information Owner, decides the system access rights for the users
- **Information/data Owner**
  - Responsible for information lifecycle activities
  - Data access decisions are best made by the information/data owner
- **Data Custodian**
  - Takes care of data on behalf of owner

Responsibility of Governing Body

- Be **informed** about information security
- Set **direction** to drive policy and strategy
- Set **priorities**
- Provide **resources** to security efforts
- Support **changes** required
- Assign **management** responsibilities
- Obtain **assurance** from internal/external audits
- Insist that security investments are **measurable** and reported on for program effectiveness

Ownership of the IS Program

- Information security **program owner** should be as **senior** as possible who is able to focus on the **management** of the security program.

- The President and CEO would not be an appropriate choice because an executive at this level is unlikely to have the time necessary to focus on security.

- **Chief Information Officer** is the most senior position who would be the strongest advocate at the executive level.

Responsibility of Management

- **Write** security policies with business input
- Getting policy **approvals** from governing body
- Setting priorities about **criticality**
- Identify **threats** and vulnerabilities
- Obtaining **resources**
- Ensure defined roles and **responsibilities**

Responsibility of Management

- **Arbitrating** disputes among team members
- Manage to implement security **infrastructures** and control frameworks (standards, guidelines, baselines, and procedures)
- Conduct periodic reviews and **tests**

Role of Security Officer

- Information security officer is **accountable** for implementing information security controls.
- IS officer must work with managers of the peer departments to ensure that security is considered throughout the project lifecycle.
- Determine the best fit with performance metrics
- Communicate risks to the management

System User

- System user is an individual that is authorized to access information systems to perform assigned duties.

- System user responsibilities include
  - adhering to organizational policies;
  - using IT resources for defined purposes only;
  - and reporting anomalous system behavior.

Role of Systems Auditor

- Information systems auditors help the organization to identify the control gaps.

- They provide an independent view of the design, implementation, and effectiveness of the controls.

- Audit results generate findings that require management response and corrective action plans to resolve the issues and mitigate the necessary risks.

Due Diligence

- **Due Diligence:** the company properly investigated all the possible **risks.**
  - performed even before starting the project

- Also includes **monitoring** the organization's practices to ensure they are meeting the security requirements.
  - Management perspective
  - Make sure that due care is being exercised

Due Care

- **Due care:** Ensuring that best **practices** are **implemented** and followed.
    - Usually performed during the execution of the projects
    - Implementation/operations perspective
    - Provides a base level/minimum protection that a reasonable person should exercise

Due Diligence & Due Care

- Due diligence is understanding the current threats and risks and due care is implementing countermeasures to provide protection from those threats.
- If a company does not practice due diligence and due care pertaining to the security of its assets, it can be legally charged with negligence and held accountable for any ramifications of that negligence.

Prudent Man Rule

- The prudent man rule requires that senior executives take personal responsibility for ensuring the due care that ordinary, prudent individuals would exercise in the same situation.

- The rule originally applied to financial matters, but the Federal Sentencing Guidelines applied them to information security matters too in 1991.