Information Assurance

Domain 1

Information Security Governance

Part B

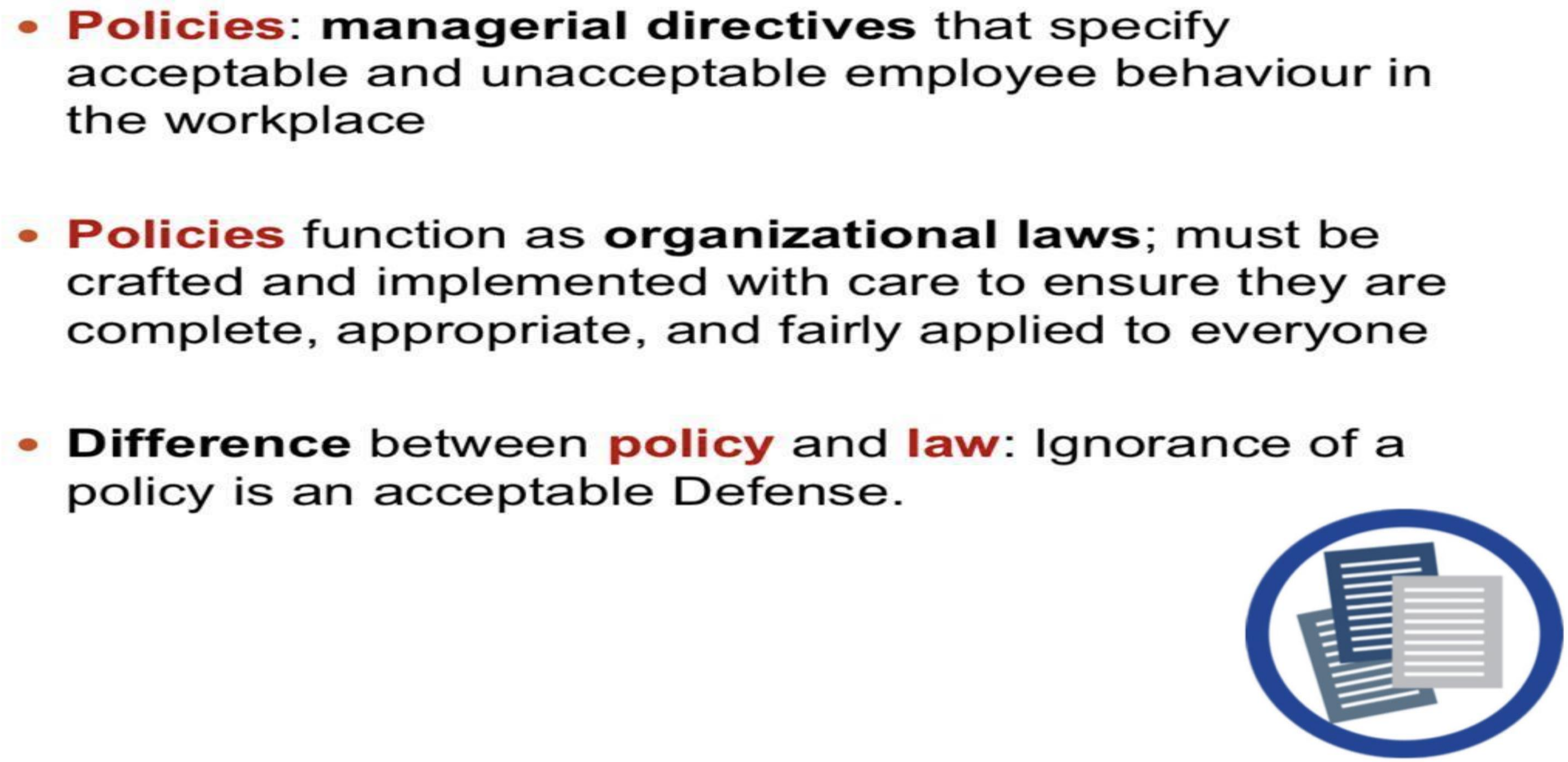
Information Security Strategy

Policy

Policies

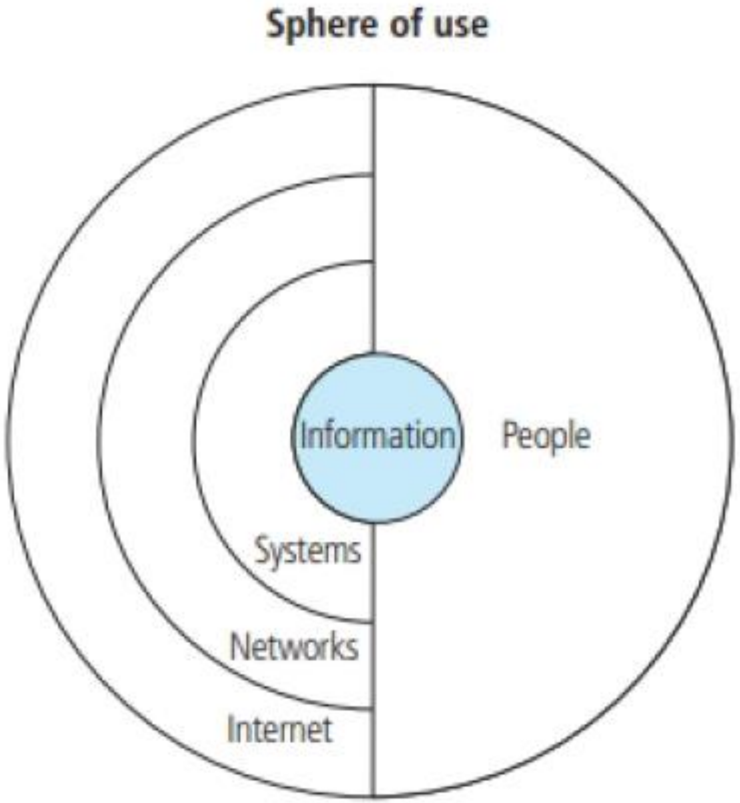
- Each policy connects to a part of the strategy
- Broad enough not to require regular revision, but should be periodically reviewed
- Approved at the highest level
- Authoritative policies pave the way for effective implementation

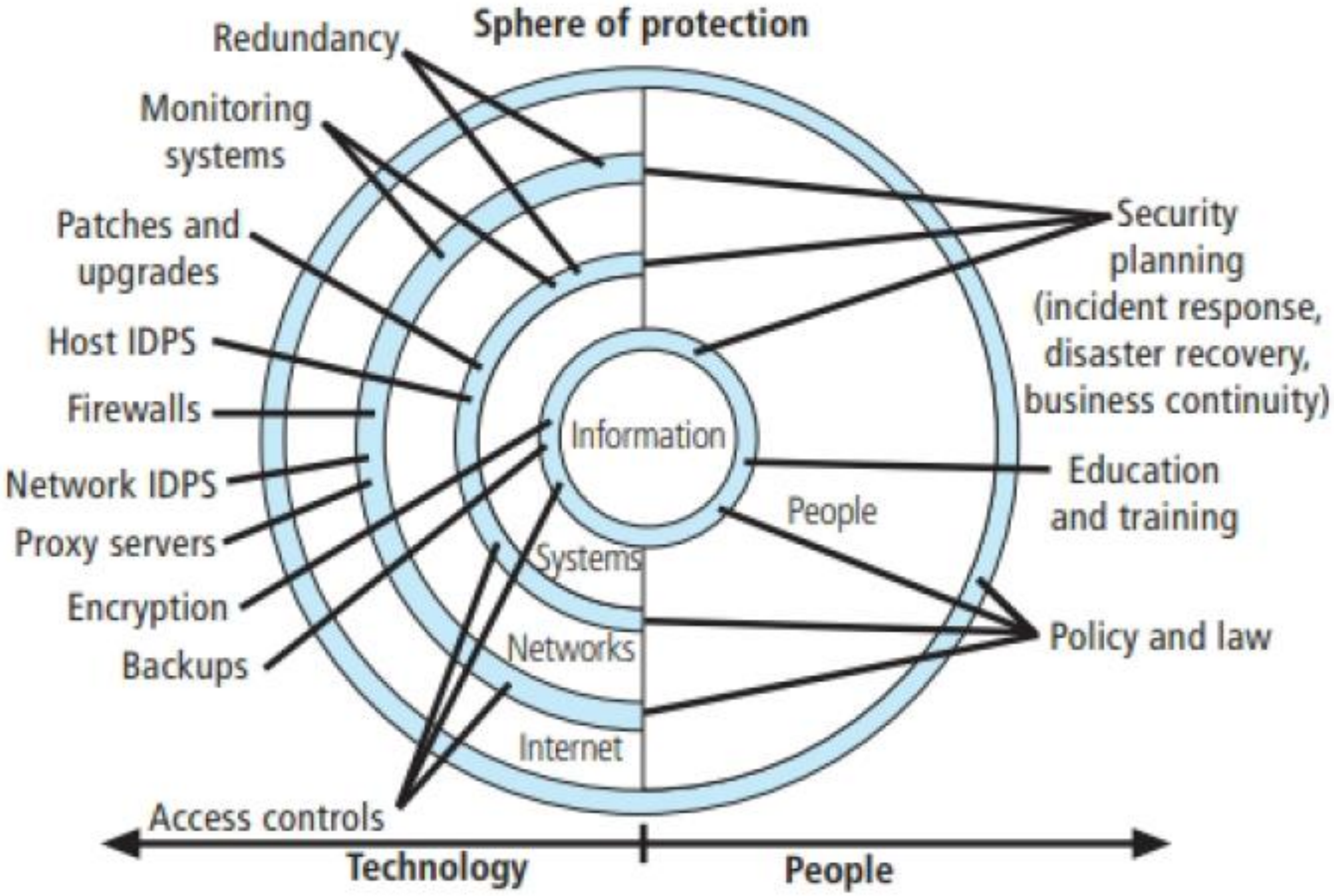
Policy



- **Policies**: **managerial directives** that specify acceptable and unacceptable employee behaviour in the workplace
- **Policies** function as **organizational laws**; must be crafted and implemented with care to ensure they are complete, appropriate, and fairly applied to everyone
- **Difference** between **policy** and **law**: Ignorance of a policy is an acceptable Defense.

Policy

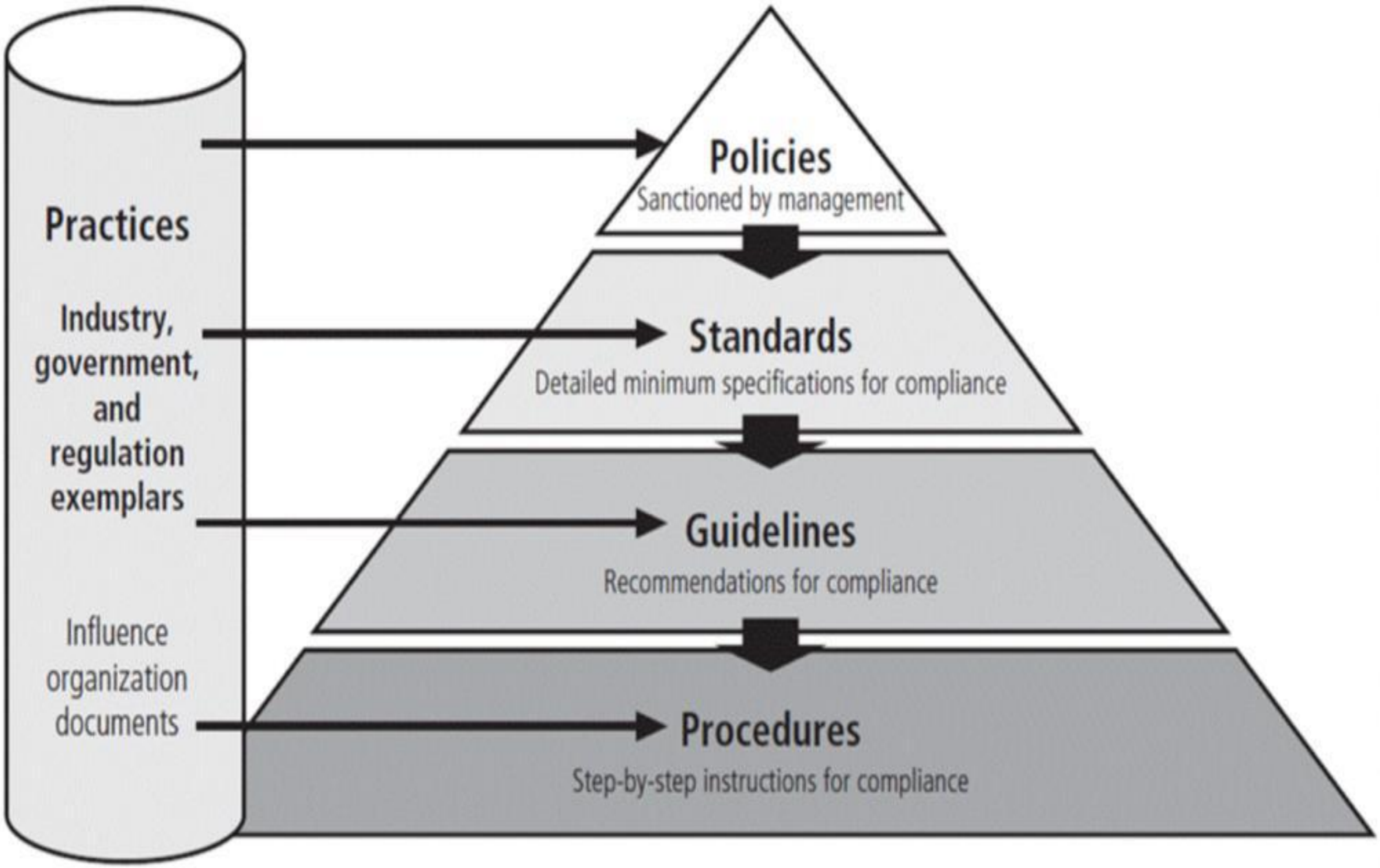

Sphere of use
Information
People
Systems
Networks
Internet


Sphere of protection
Redundancy
Monitoring systems
Patches and upgrades
Host IDPS
Firewalls
Network IDPS
Proxy servers
Encryption
Backups
Access controls
Information
People
Systems
Networks
Internet
Security planning (incident response, disaster recovery, business continuity)
Education and training
Policy and law
Technology
People

Policy- As Foundation for Planning

- **Policy** functions as organizational **law** that dictates acceptable and unacceptable behavior.
- **Standards**: more detailed statements of what must be done to comply with policy
- **Practices, procedures, and guidelines** effectively explain how to comply with policy.
- For a policy to be effective, it must be properly **disseminated, read, understood**, and **agreed** to by all members of the organization, and uniformly enforced.

Policy


Practices
Industry, government, and regulation exemplars
Influence organization documents
Policies
Sanctioned by management
Standards
Detailed minimum specifications for compliance
Guidelines
Recommendations for compliance
Procedures
Step-by-step instructions for compliance

Policies

- Attributes of good policies:
  - Should capture the intent, expectations and direction of management
  - Should state only one general security mandate
  - Must be clear and easily understood
  - Includes just enough context to be useful
  - Rarely number more than two dozen in total

Metrics and Measurement

- Security metrics tell us about the state of security relative to a reference point
- They show whether our security efforts are improving, staying the same, or getting weaker

Metrics and Measurement

- Metrics should be SMART:
  - Specific
  - Measurement
  - Attainable
  - Relevant
  - Timely

Metrics and Measurement

- Metrics should be SMART:
  - **Specific:**
    - The metric should clearly define what is being measured
    - Instead of improve security, use “reduce phishing incidents.”
    - Specific goal: Number of phishing emails reported by employees per month.
  - **Measurement:**
    - You should be able to quantify or track it with data.
    - Measure “percentage of systems with latest security patches installed.” (e.g., 95% patched systems).

Metrics and Measurement

- Metrics should be SMART:
  - **Attainable**
    - The goal or target should be realistic, something that can actually be achieved with available resources.
    - Setting a target to “achieve 100% system patching within 24 hours” may not be possible. A better attainable goal is “Achieve 90% patching within 7 days of release.”
  - **Relevant**
    - The metric should connect to organizational or security goals, not just random data.
    - Tracking “number of firewall rules” isn’t very relevant to business risk, but measuring “number of successful intrusions prevented” is directly tied to security objectives.

Metrics and Measurement

- Metrics should be SMART:
  - **Timely**
    - The metric should be measured and reviewed at the right time intervals (daily, weekly, quarterly).
    - “Conduct quarterly reviews of user access rights.” This keeps the data fresh.

These metrics connect security performance with business success.

Metrics at the Strategic Level

- Key goal indicators (KGIs) and key performance indicators (KPIs) can be useful for process or service goals.
- High-level metrics related to implementing a governance program:
  - Alignment with business goals and objectives
  - Management of risk to acceptable levels
  - Effective management of resources
  - Performance and value delivery

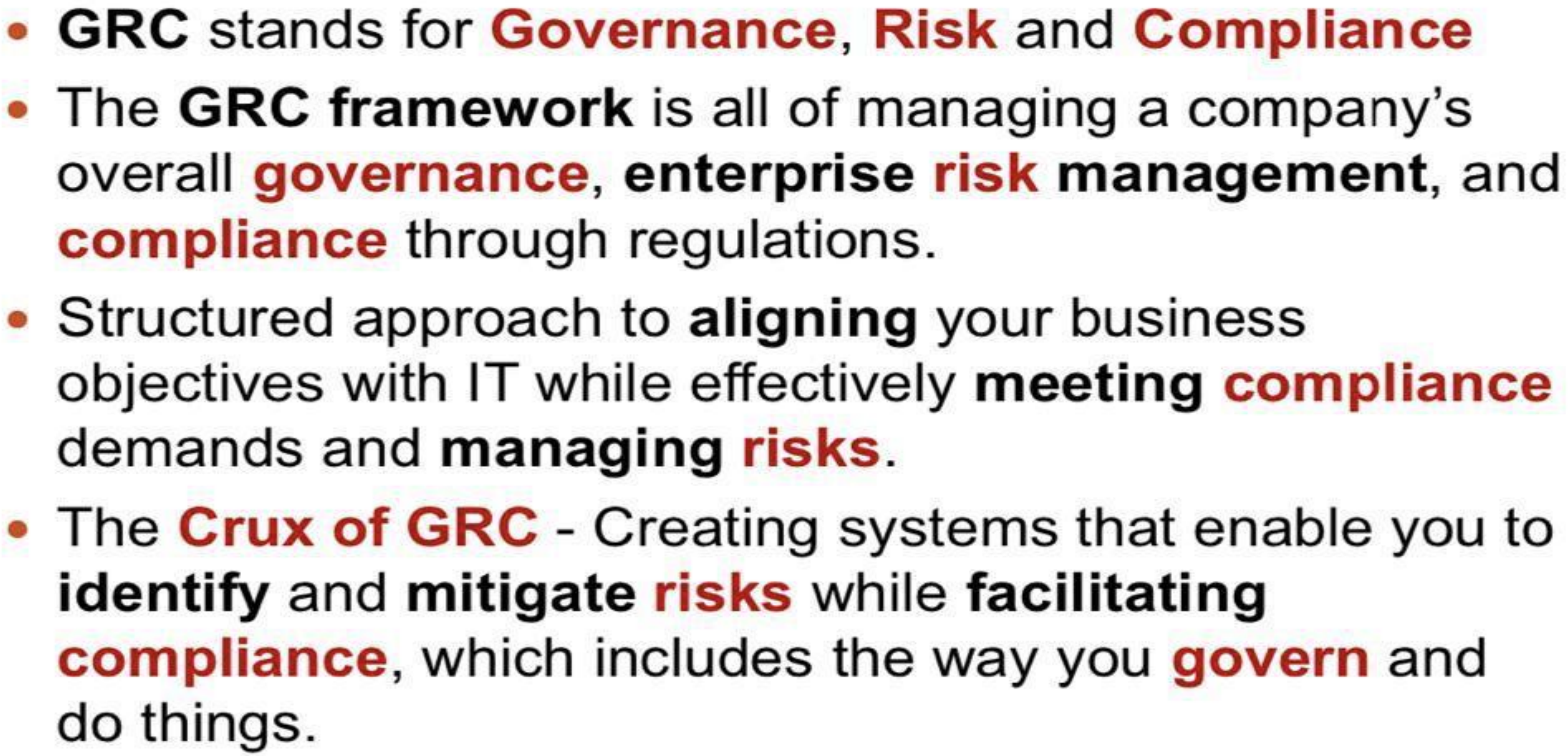
Risk Management Metrics

- Indicators of appropriate risk management include:
  - Defined risk appetite and tolerance
  - Process for management of adverse impacts
  - Trends in periodic risk assessment and impacts
  - Completeness of asset inventory
  - Ratio of security incidents from known to unknown security risks

Performance Measurement

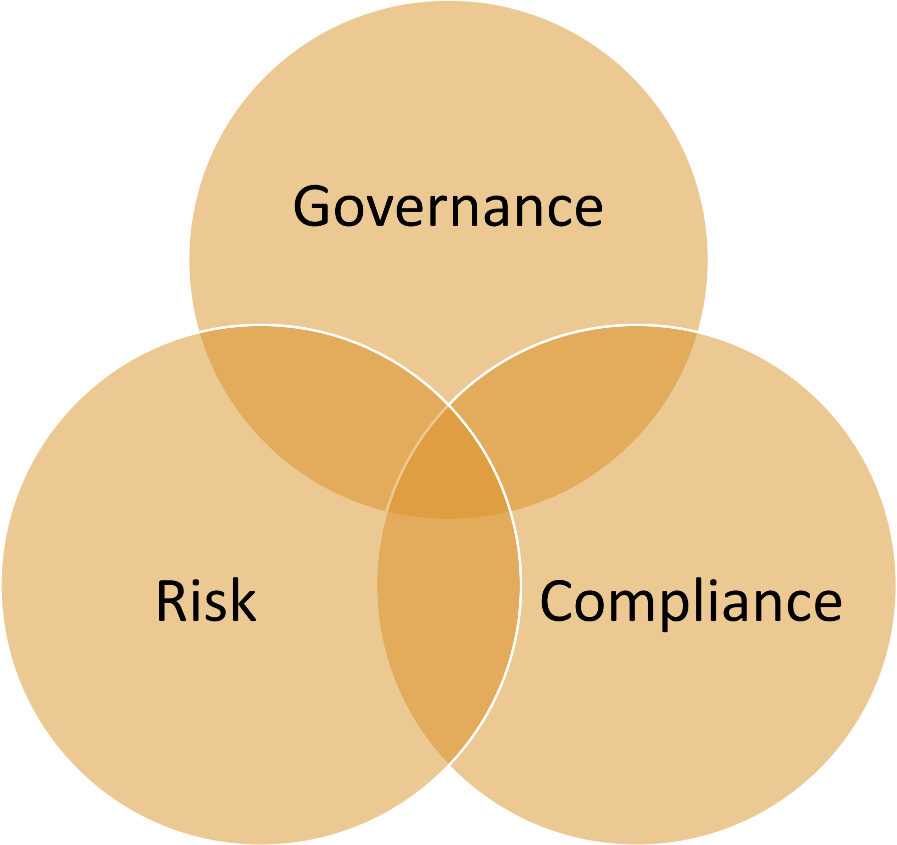
- Indicators of effective performance measurement include:
  - The time required to detect and report security events
  - The number and frequency of unreported incidents
  - Benchmarking comparable organizations for costs and effectiveness
  - Knowledge of evolving and impending threats
  - Methods of tracking evolving risk
  - Consistency of log review practices

GRC Framework



- **GRC** stands for **Governance**, **Risk** and **Compliance**
- The **GRC framework** is all of managing a company's overall **governance**, **enterprise risk management**, and **compliance** through regulations.
- Structured approach to **aligning** your business objectives with IT while effectively **meeting compliance** demands and **managing risks**.
- The **Crux of GRC** - Creating systems that enable you to **identify** and **mitigate risks** while **facilitating compliance**, which includes the way you **govern** and do things.

Governance, Risk and Compliance (GRC)



- GRC is an integrated assurance process
- Convergence can exist independently across different business functions

Home Task

- List down the name and reference numbers of the Information Security and Information Security Governance Framework, Standards, Guidelines, and Technical Report.
- Prepare a brief report on COBIT Framework - (1 – 2 pages)

Thanks a lot