

Security Governance Principles

Dr. Shahzada Khurram

○ Least Privilege and Need to Know.

- **Least Privilege** – (Minimum necessary access) Give users/systems exactly the access they need, no more, no less.
- **Need to Know** – Even if you have access, if you do not need to know, then you should not access the data.

○ Non-repudiation.

- A user cannot deny having performed a certain action. This uses both Authentication and Integrity.

○ Subject and Object.

- **Subject** – (Active) Most often users but can also be programs – Subject manipulates Object.
- **Object** – (Passive) Any passive data (both physical paper and data) – Object is manipulated by Subject.
- Some can be both at different times, an active program is a subject; when closed, the data in program can be object.

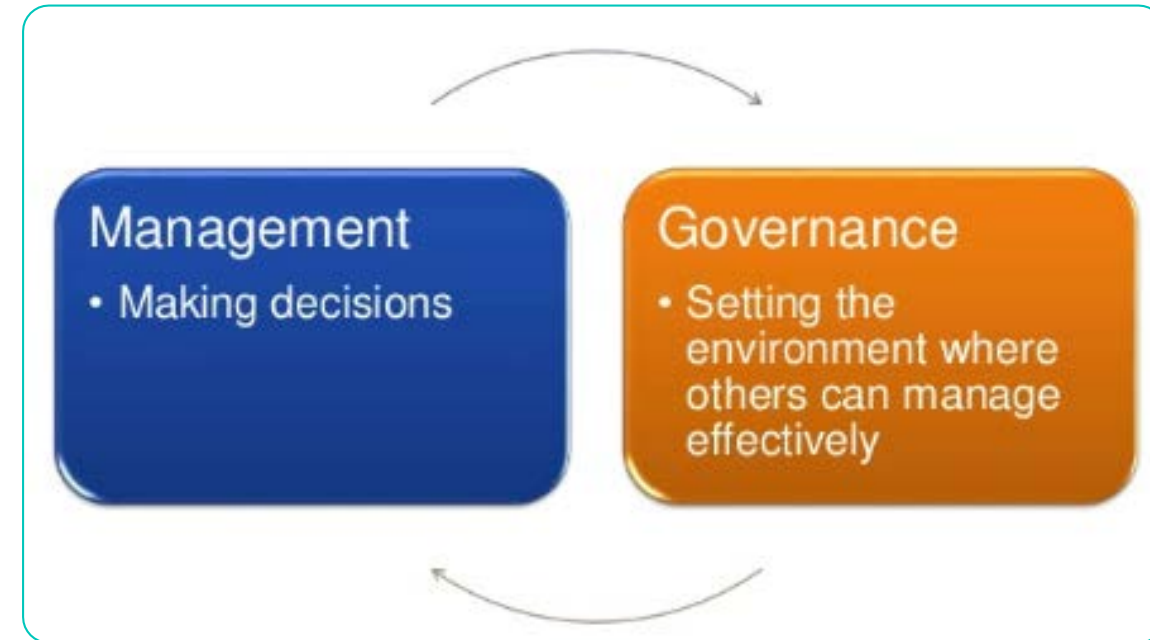
Governance vs. Management

○ **Governance** – This is C-level Executives (Not you).

- Stakeholder needs, conditions and options are evaluated to define:
- Balanced agreed- upon enterprise objectives to be achieved.
- Setting direction through prioritization and decision making.
- Monitoring performance and compliance against agreed-upon direction and objectives.
- Risk appetite – Aggressive, neutral, adverse.

○ **Management** – How do we get to the destination (This is you).

- Plans, builds, runs and monitors activities in alignment with the direction set by the governance to achieve the objectives.
- Risk tolerance – How are we going to practically work with our risk appetite and our environment.



Top-Down vs. Bottom-Up Security Management and Organization structure

- **Bottom-Up:** IT Security is seen as a nuisance and not a helper, often change when breaches happen.
- **Top-Down:** IT leadership is on board with IT Security, they lead and set the direction. (The exam).
- **C-Level Executives (Senior Leadership) Ultimately Liable.**
 - **CEO:** Chief Executive Officer.
 - **CSO:** Chief Security Officer.
 - **CIO:** Chief Information Officer.
 - **CFO:** Chief Financial Officer.

Normal organizations obviously have more C-Level executives, the ones listed here you need to know.





Thank you