# Security components

## Summary

In this class exercise, we will introduce the purpose of security components, define the types of security components, and provide examples of them. This should be performed without the aid of any electronic device.

## Prerequisites

* None

## Details

* Study the security concepts and relationships diagram below. Discuss each node and provide an example for each. Circle the node where security components fit in.



Figure -CCMB-2012-09-001

* Owners
* Threat agents
* Threats
* Risk
* Assets
* Countermeasures
* Consider how security requirements (security goals or expectations) could be used to mitigate risks from vulnerabilities. Provide some examples, to share with the class, of security requirements that a software maker (e.g., Microsoft or Apple) might have for one of its products.
* Consider how security policy (defines what is allowed and not allowed, and how security goals and expectations are achieved) could be used to mitigate risks from vulnerabilities. Provide some examples, to share with the class, of policy that a software maker (e.g., Microsoft or Apple) might have for one of its products.
* Consider how security mechanisms (enforce policy via tools, procedures, and other means) could be used to mitigate risks from vulnerabilities. Provide some examples, to share with the class, of security mechanisms and their intended use that a software maker (e.g., Microsoft or Apple) might have for one of its products.
* Consider how company leaders ensure security policy is being enforced. Provide some examples, to share with the class, of security assurance that a software maker (e.g., Microsoft or Apple) might use while implementing one of its products.
* Consider the diagram below which represents a process for continually updating security policy. Why should policy be updated in this manner?

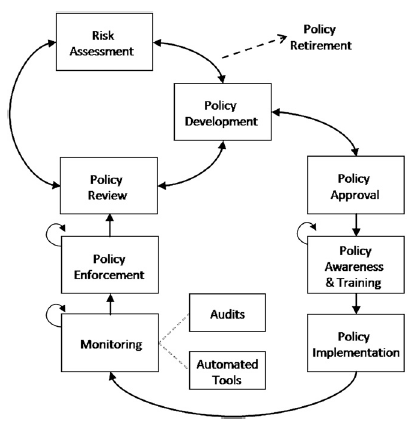


Figure 2-Information security policy as a process (Knapp et al. 2009)

### Definitions

* Security requirements-define security goals (Bishop 2003)
  + They answer the question, “What do you expect security to do for you?”
* Security policy-defines the meaning of security (Bishop 2003)
  + Specifies what actions and states are allowed or disallowed by the product or service at particular times
  + Includes security rules for system developers, testers, users, components, and information
  + It answers the question, “What steps do you take to reach the goal set out above?”
* Security mechanisms-enforce security policy (Bishop 2003)
  + The system must provide mechanisms adequate for enforcing the policy
  + They answer the question, “What tools, procedures, and other ways do you use to ensure that the above steps are followed?”
* Security assurance-measures how well requirements conform to needs, policy conforms to requirements, and mechanisms implement the policy (Bishop, 2003)
  + Answers the questions, “Does a system’s set of mechanisms, taken as a whole, correctly implement the security policy?”, “Does the system’s security policy conform to requirements?”, and “Do the security requirements conform to and meet all the system’s security needs?”