Ontological Approach toward Cybersecurity in Cloud Computing

Takeshi Takahashi, Youki Kadobayashi

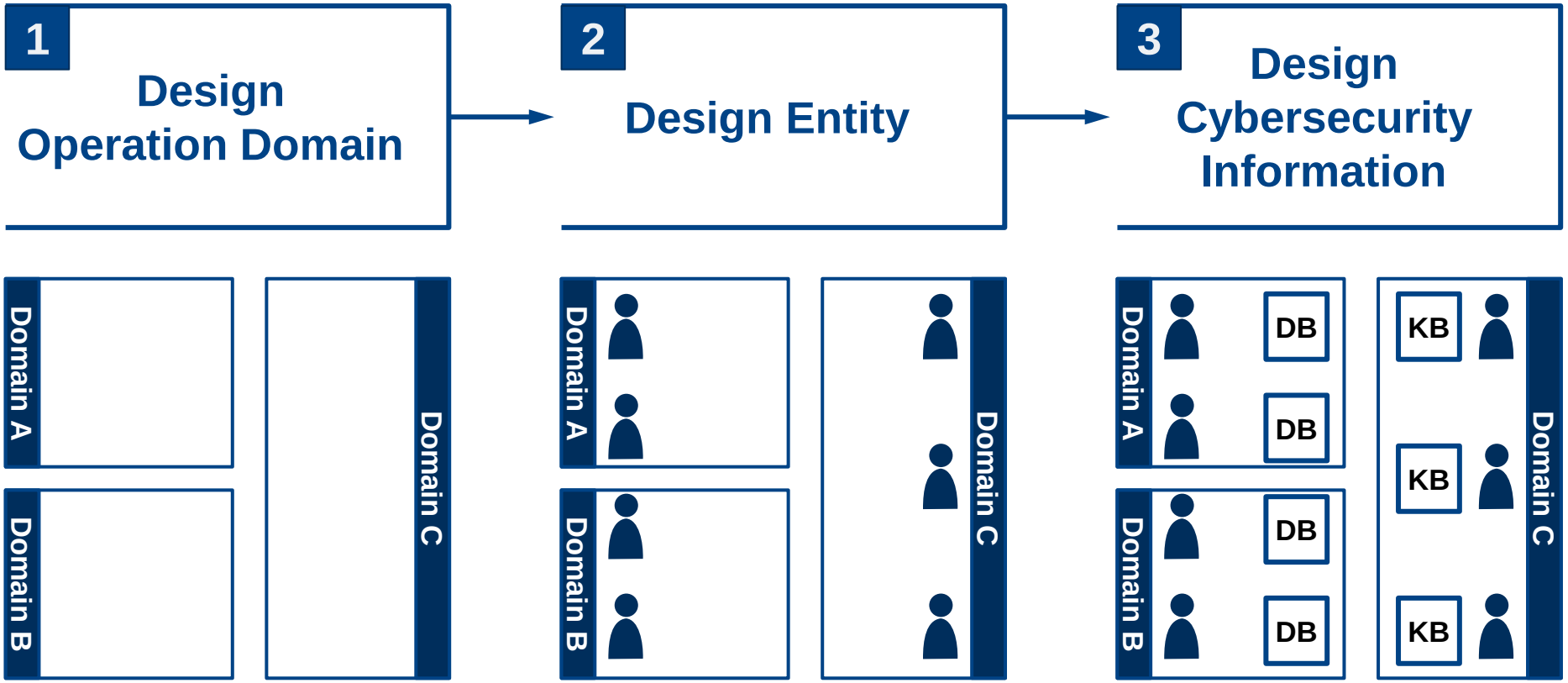
NICT
Tokyo, Japan

Focus of today's discussion

This presentation discusses needed cybersecurity information for cloud computing based on an ontology

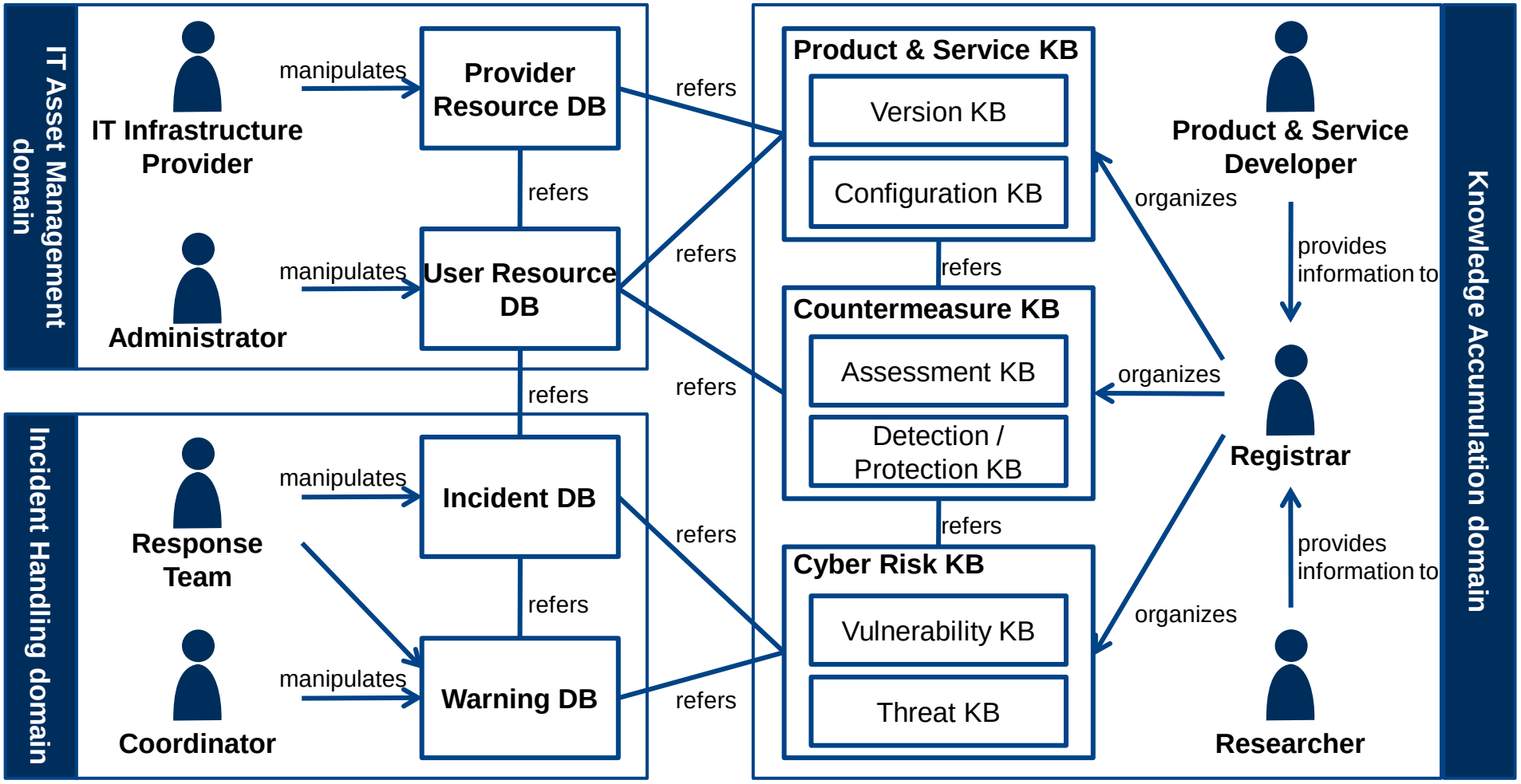
We built an ontology following the 3-step approach

Three steps to build the ontology



Source : “Ontological Approach toward Cybersecurity in Cloud Computing,” ACM SIN, September 2010

This ontology could be used as a basis of discussing cybersecurity issues

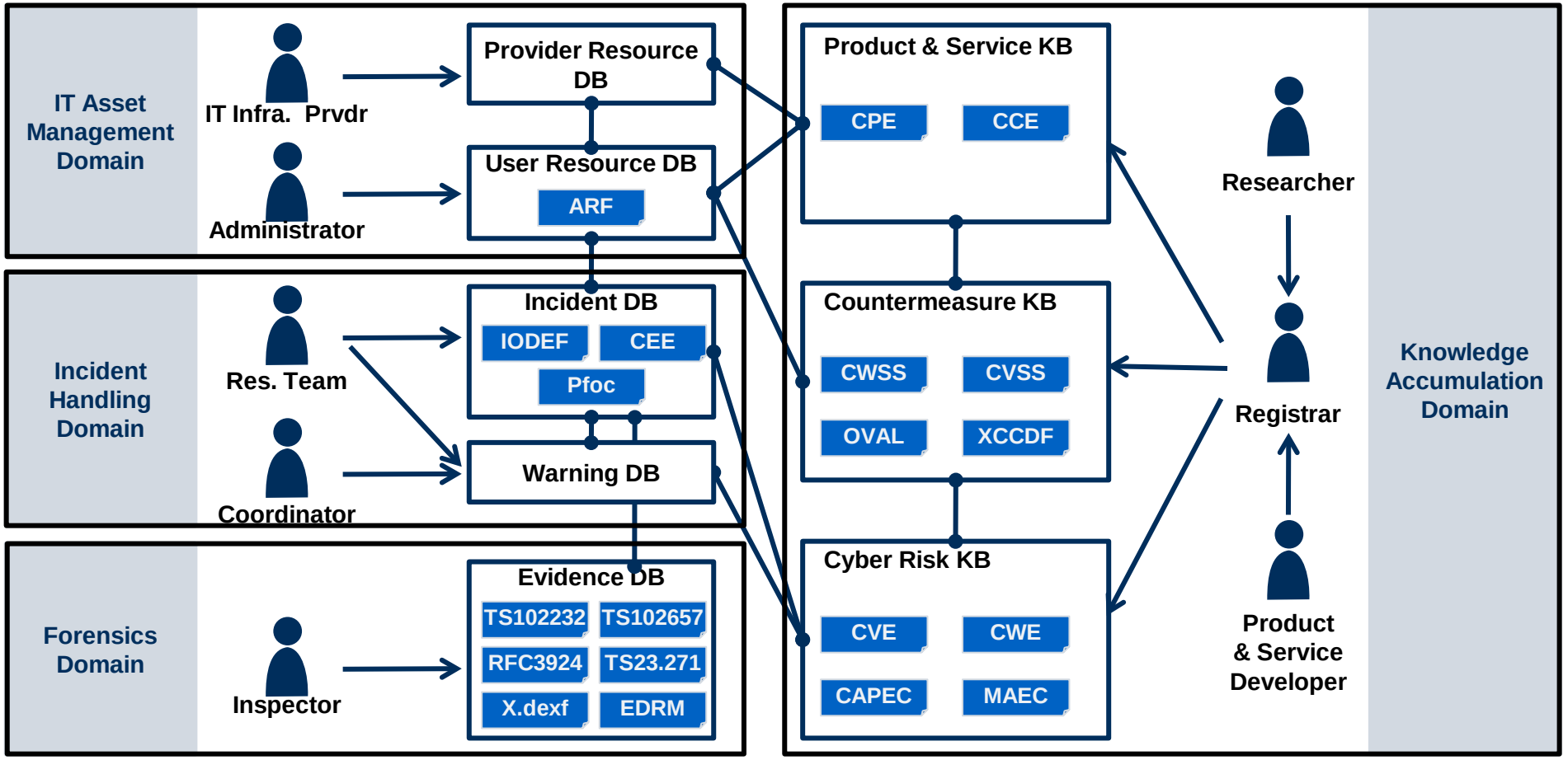


DB: Database KB: Knowledge base

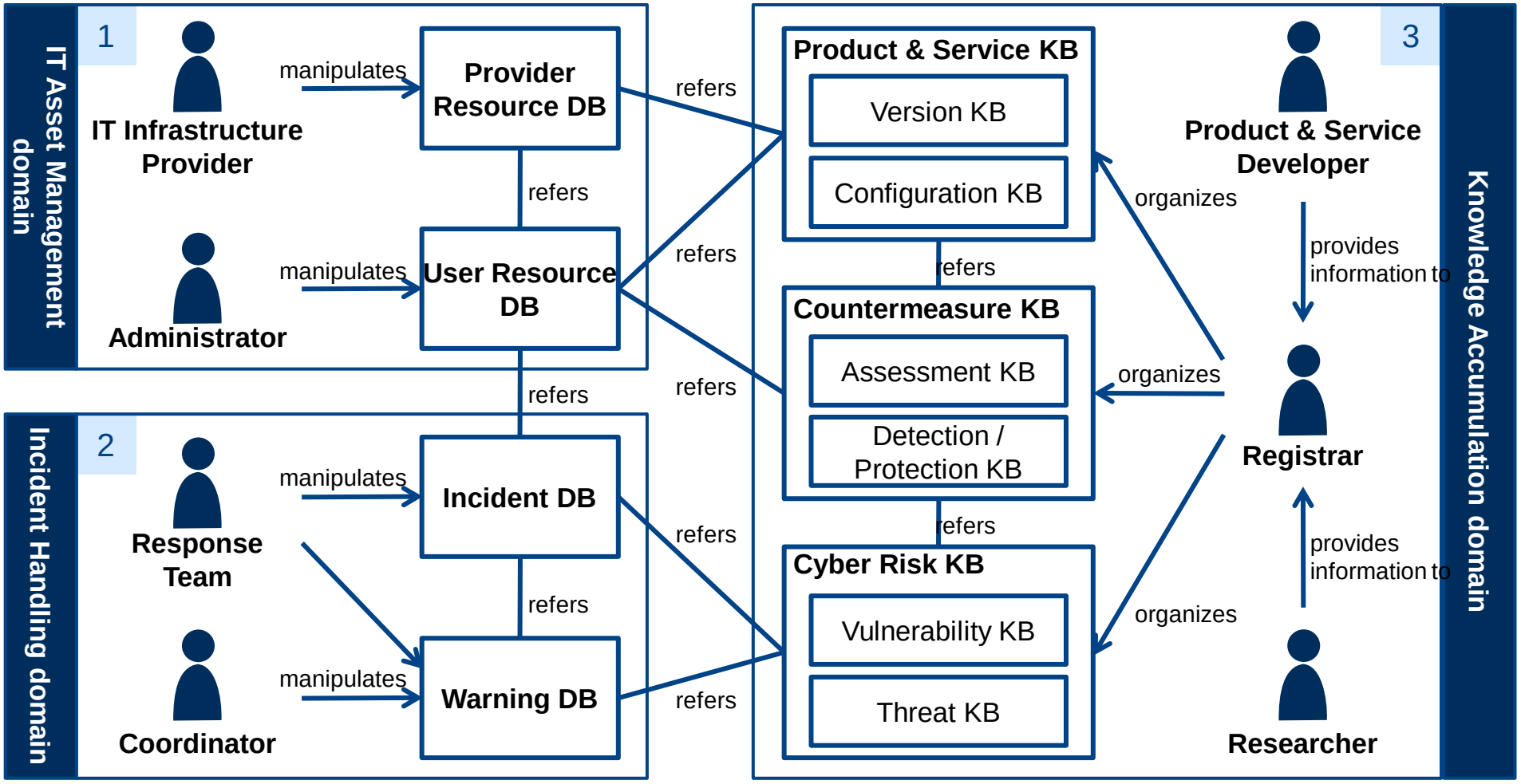
Source : “Ontological Approach toward Cybersecurity in Cloud Computing,” ACM SIN, September 2010

The ontology is referenced by X.1500 and is utilized as a basis of reviewing the orchestration of existing works

Mapping of cybersecurity information standards

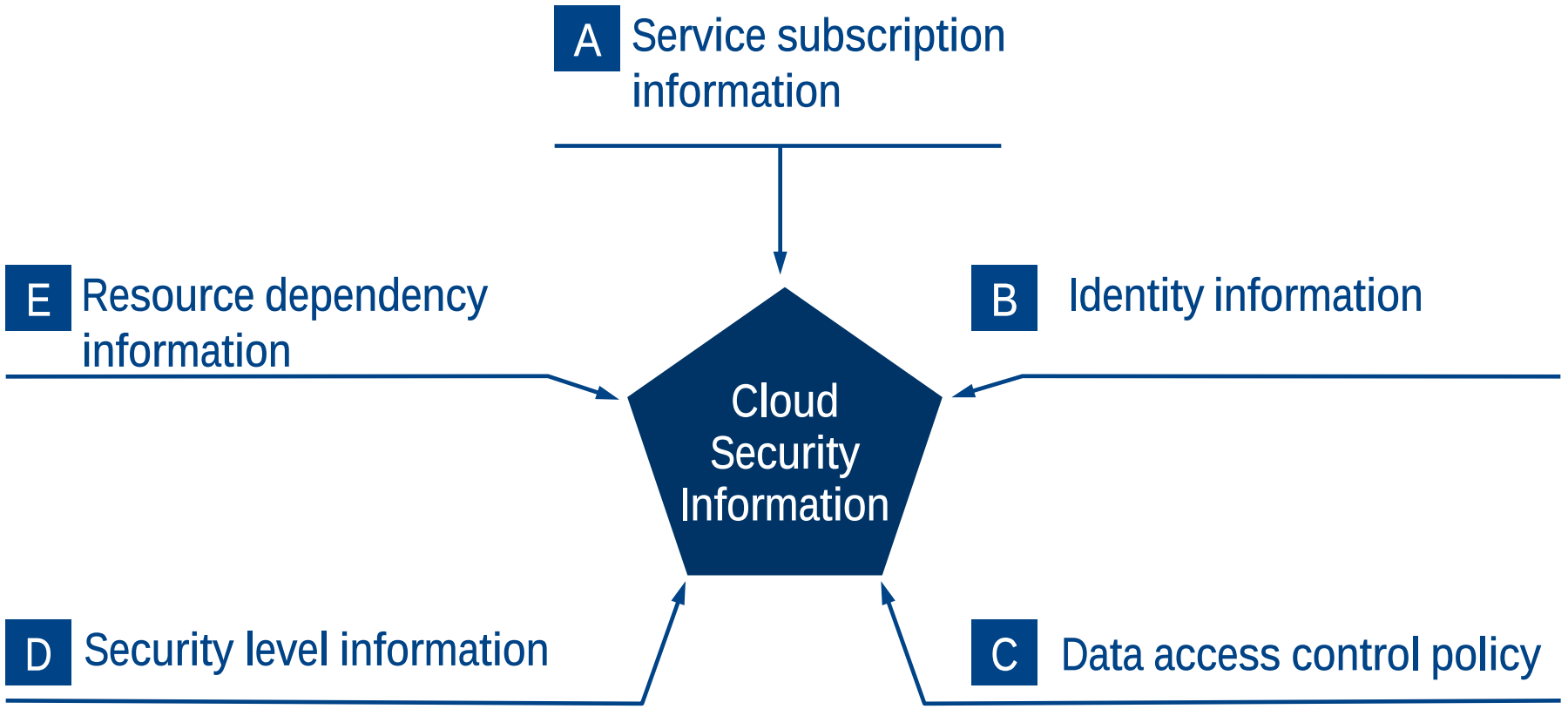


In this presentation, we would like to discuss some of the issues toward cybersecurity in cloud computing



DB: Database KB: Knowledge base

Needed information in the User Resource DB



* this presentation omit discussing Provider Resource DB due to the interest of time

Source : “Ontological Approach toward Cybersecurity in Cloud Computing,” ACM SIN, September 2010

Needed information in the Incident Handling domain

Incident DB

Data provenance	• Log of any data manipulation
Data placement log	• Change log of the mapping between logical and physical data location
Data incident/event information	• Incident/event information on data apart from asset

Warning DB

Warning to indirect users	• Warnings need to be provided to indirect users of warned resources
Warning on data incident/event	• Warning of incident/event on data apart from asset

Source : “Ontological Approach toward Cybersecurity in Cloud Computing,” ACM SIN, September 2010

Needed information in the Knowledge Accumulation domain

Cyber Risk KB

Configuration vulnerability

- Vulnerabilities caused by mis-configuration of resources and their combinations

Human factors causing risks

- Human vulnerabilities causing cyber risks (the weakest links are humans)

Countermeasure KB

Methodologies to evaluate cybersecurity

- Existing methodologies such as CVSS need to be advanced further to cope with cloud computing

Product&Service KB

Cloud service enumeration /taxonomy

- Naming of cloud services and the enumeration and taxonomy

Service configuration enumeration /taxonomy

- Naming of service configuration and the enumeration and taxonomy

Source : “Ontological Approach toward Cybersecurity in Cloud Computing,” ACM SIN, September 2010

In order to maintain cybersecurity in cloud computing, further research and standardization activities are needed

- Based on the CYBEX ontology, we raised some cybersecurity issues to accommodate cloud computing
  - Resource dependency, identity, data provenance, data placement change log, data incident, human factors, service enumeration/taxonomy, etc.
- In order to accommodate cloud computing, further research and standardization activities are needed, and CYBEX / CYBEX ontology is a good starting point for discussing them
- Some more details are available at “Ontological Approach toward Cybersecurity in Cloud Computing” (ACM SIN, September 2010)