Sistem Access Control & Metodologi

Dr. Mohammad Iqbal
Thanks to Jeff Smith, CISSP et al
Defenisi Access Controls

• **Access control** is the collection of mechanisms that permits managers of a system to exercise a directing or restraining influence over the behavior, use, and content of a system. It permits management to specify **what users** can do, **which resources** they can access, and **what operations** they can perform on a system.
Lingkup Materi Access Controls

- Konsep Access control
- Metodologi Access control
- Implementation within centralized and decentralized environments across the enterprise’s computer systems.
- Access control techniques, detective and corrective measures to understand the potential risks, vulnerabilities, and exposures.
Overview Access Control

- **Access Controls**: The security features that control how users and systems communicate and interact with one another.

- **Access**: The flow of information between subject and object

- **Subject**: An active entity that requests access to an object or the data in an object

- **Object**: A passive entity that contains information
## Terminologi dalam Akses Kontrol

<table>
<thead>
<tr>
<th>Accountable person who desires access</th>
<th>User or process acting for person</th>
<th>Potential actions that may be applied</th>
<th>Resource subject to access control</th>
</tr>
</thead>
<tbody>
<tr>
<td>Secure Computing: Threats and Safeguards, 1997, Rita C. Summers</td>
<td>Subject</td>
<td>Subject</td>
<td>Rights</td>
</tr>
<tr>
<td>Computer Security, 1996, John Carroll</td>
<td>User Identifier</td>
<td>User Identifier</td>
<td>Access Control List</td>
</tr>
<tr>
<td>Computer Communications Security, 1994, Warwick Ford</td>
<td>User</td>
<td>Initiator</td>
<td>Access Permissions</td>
</tr>
<tr>
<td>X/Open Distributed Security Framework, 1994, The Open Group</td>
<td>User</td>
<td>Initiator</td>
<td>Initiator ACL Target ACL</td>
</tr>
<tr>
<td>CORBA Security Services Specification 1.0, 1996, Object Management Group</td>
<td>Principal, Subject</td>
<td>Initiator, Client, Principal</td>
<td>Access policy rights, Privilege attributes, Control attributes</td>
</tr>
</tbody>
</table>
The three main security principles also pertain to access control:

- Availability
- Integrity
- Confidentiality
Prinsip Keamanan: Mengukur Nilai informasi – Segitiga CIA

The value of information comes from the characteristics it possesses.
Prinsip Keamanan : Model ISO untuk Otorisasi

Principal

Access Control
Enforcement Function

Identity, Access Request
Additional Attributes

Access
Decision Cache

Resource

Request, Identity, Attributes

Audit Logs

Access Control Decision Function

Environmental, Resource, & Principal Attributes; Identifiers

Relatively Dynamic

Relatively Static

Policy Admin

Rules
Prinsip Keamanan : Konsep Manajemen Privilege

Identification

Who are you?

Authentication

Prove it!

Authorization

Here’s your stuff...

- **Identification**: The presentation of an identifier so that the system can recognize and distinguish the presenter from other principals.
- **Authentication**: The exchange of information in order to verify the claimed identity of a principal.
- **Authorization**: The granting of rights, including access, to a principal, by the proper authority.

**Principal**: An entity (people, devices, applications, etc.) whose identity can be authenticated.

Reference: Open Group XDSF (X/Open Distributed Security Framework), ISO 10181-3
Identification, Authentication, and Authorization are distinct functions.

1. Identification
2. Authentication
3. Authorization

Identity Management: A broad term to include the use of different products to identify, authenticate, and authorize users through automated means.
Identification

- Method of establishing the subject’s (user, program, process) identity.
  - Use of user name or other public information.
  - Know identification component requirements.

- Identification: unproven assertion of identity
  - “My name is...”
  - Userid
**Authentication**

- Method of proving the identity.
  - Something a person is, has, or does.
  - Use of biometrics, passwords, passphrase, token, or other private information.

**Strong Authentication is important**

- Authentication: proven assertion of identity
  - Userid and password
  - Userid and PIN
  - Biometric
### Passwords

- User name + password most common identification, authentication scheme.
- Weak security mechanism, must implement strong password protections
- Implement Clipping Levels
Techniques to attack passwords

- Electronic monitoring
- Access the password file
- Brute Force Attacks
- Dictionary Attacks
- Social Engineering

Know difference between a password checker and a password cracker.
Passphrase

- Is a sequence of characters that is longer than a password.
- Takes the place of a password.
- Can be more secure than a password because it is more complex.
One Time Passwords (aka Dynamic Passwords)

- Used for authentication purposes and are only good once.
- Can be generated in software (soft tokens), or in a piece of hardware
Two types of Token Devices (aka Password Generator)

• Synchronous
  » Time/event Based
  » Using one-time password or hashed values
  » Authentication server knows expected value from the token
  » Counter Synchronization

• Asynchronous

Know the different types of devices and how they work.
Token: Two Factor Authentication

- First factor: what user knows
- Second factor: what user has

Without the second factor, user cannot log in
Token: Two Factor Authentication
Smart Cards and Memory Cards

• Memory Cards: Holds but cannot process information.
• Smart Cards: Holds and can process information.
  » Contact
  » Contactless
    – Hybrid
    – Combi
Attacks on Smart Cards

- Fault Generation
- Microprobing
- Side Channel Attacks (nonintrusive attacks)
  - Differential Power Analysis
  - Electromagnetic Analysis
  - Timing
  - Software attacks
Hashing & Encryption

- Hash or encrypting a password to ensure that passwords are not sent in clear text (means extra security)

- Windows environment, know syskey modes.

- Salts: Random values added to encryption process for additional complexity.
Password Hashes

- LM hash is weak, no longer used in Win 7
- NT hash is stronger, but not salted

Cryptographic Keys
  • Use of private keys or digital signatures to prove identity

Private Key

Digital Signature
  • Beware digital signature vs. digitized signature.
Biometrics

- Verifies an identity by analyzing a unique person attribute or behavior (e.g., what a person “is”).

- Most expensive way to prove identity, also has difficulties with user acceptance.

- Many different types of biometric systems, know the most common.
• Most common biometric systems:
  - Fingerprint
  - Palm Scan
  - Hand Geometry
  - Iris Scan
  - Signature Dynamics
  - Keyboard Dynamics
  - Voice Print
  - Facial Scan
  - Hand Topography
Biometric systems can be hard to compare.

- Type I Error: False rejection rate.
- Type II Error: False acceptance rate.
  - This is an important error to avoid.

Crossover Error Rate
Authorization

• Determines that the proven identity has some set of characteristics associated with it that gives it the right to access the requested resources.
Access Criteria can be thought of as:

- Roles
- Groups
- Location
- Time
- Transaction Types
Authorization concepts to keep in mind:

- Authorization Creep
- Default to Zero
- Need to Know Principle
- Access Control Lists
• Problems in controlling access to assets:
  • Different levels of users with different levels of access
  • Resources may be classified differently
  • Diverse identity data
  • Corporate environments keep changing
Solutions that enterprise wide and single sign on solutions supply:
- User provisioning
- Password synchronization and reset
- Self service
- Centralized auditing and reporting
- Integrated workflow (increase in productivity)
- Regulatory compliance
- **Single Sign On Capabilities**
  - Allow user credentials to be entered one time and the user is then able to access all resources in primary and secondary network domains

- **SSO technologies include:**
  - Kerberos
  - Sesame
  - Security Domains
  - Directory Services
  - Dumb Terminals
Authentication

• Use a unique identifier—
  » Example: user ID, Account number, PIN
• 3 main datum used for authentication
  » Something requester know
    - Passwords
    - Pass-phrases
  » Something the requester is
    - Biometrics
    - Physical characteristics
  » Something the requester has
    - Tokens (one-time passwords, time synchronized token)
    - Smart Cards
    - USB Tokens

Authorization

Accounting
Access Control Models

Three Main Types

1. Discretionary
2. Mandatory
3. Non-Discretionary (Role Based)
Model Access Control

- **Discretionary Access Control (DAC)**
  - A system that uses discretionary access control allows the owner of the resource to specify which subjects can access which resources.
  - Access control is at the discretion of the owner.
Model Access Control

- **Mandatory Access Control (MAC)**
  - Access control is based on a security labeling system. Users have security clearances and resources have security labels that contain data classifications.
  - This model is used in environments where information classification and confidentiality is very important (e.g., the military).
Non-Discretionary (Role Based) Access Control Models

- Role Based Access Control (RBAC) uses a centrally administered set of controls to determine how subjects and objects interact.
- Is the best system for an organization that has high turnover.
Teknologi Access Control

- There are a number of different access controls and technologies available to support the different models.
  - Rule Based Access Control
  - Constrained User Interfaces
  - Access Control Matrix
  - Content Dependent Access Control
  - Context Dependent Access Control
Rule Based Access Control

- Uses specific rules that indicate what can and cannot happen between a subject and an object.
- Not necessarily identity based.
- Traditionally, rule based access control has been used in MAC systems as an enforcement mechanism.
Teknologi Access Control

- **Constrained User Interfaces**
  - Restrict user’s access abilities by not allowing them certain types of access, or the ability to request certain functions or information

- **Three major types**
  - Menus and Shells
  - Database Views
  - Physically Constrained Interfaces
Teknologi Access Control

- **Access Control Matrix**
  - Is a table of subjects and objects indicating what actions individual subjects can take upon individual objects.

- **Two types**
  - Capability Table (bound to a subject)
  - Access Control List (bound to an object)
<table>
<thead>
<tr>
<th>Principals</th>
<th>A</th>
<th>B</th>
<th>C</th>
<th>D</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alice</td>
<td>READ</td>
<td>WRITE</td>
<td>READ</td>
<td>READ</td>
</tr>
<tr>
<td>Bob</td>
<td></td>
<td>READ</td>
<td>WRITE</td>
<td>WRITE</td>
</tr>
<tr>
<td>Eve</td>
<td></td>
<td></td>
<td>READ</td>
<td>WRITE</td>
</tr>
<tr>
<td>Alpha 1</td>
<td>READ</td>
<td>READ</td>
<td>READ</td>
<td>READ</td>
</tr>
<tr>
<td>...</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Alpha n</td>
<td>READ</td>
<td>READ</td>
<td>READ</td>
<td>READ</td>
</tr>
<tr>
<td>Alpha Group</td>
<td>READ</td>
<td>READ</td>
<td>READ</td>
<td>READ</td>
</tr>
<tr>
<td>Backup</td>
<td>READ</td>
<td>READ</td>
<td>READ</td>
<td>READ</td>
</tr>
</tbody>
</table>

**Access Control System**
Bob carries around Identity
AZN System checks
Principal identity

**Capability Based System**
Bob carries around Capability List
AZN System checks
Resource identity
Teknologi Access Control

- **Content Dependent Access Control:** Access to an object is determined by the content within the object.

- **Context Based Access Control:** Makes access decision based on the context of a collection of information rather than content within an object.
Teknologi Access Control
Administrasi Access Control

- First an organization must choose the access control model (DAC, MAC, RBAC).

- Then the organization must select and implement different access control technologies.

- Access Control Administration comes in two basic forms:
  - Centralized
  - Decentralized
Centralized Access Control Administration:

- One entity is responsible for overseeing access to all corporate resources.
- Provides a consistent and uniform method of controlling access rights.
  - Protocols: Agreed upon ways of communication
  - Attribute Value Pairs: Defined fields that accept certain values.

Types of Centralized Access Control

- Radius
- TACAS
- Diameter
Administrasi Access Control

- Decentralized Access Control Administration:
  - Gives control of access to the people who are closer to the resources
  - Has no methods for consistent control, lacks proper consistency.
Access controls can be implemented at various layers of an organization, network, and individual systems.

Three broad categories:
- Administrative (aka Management)
- Physical (aka Operational)
- Technical (aka Logical)
Metode Access Control

- **Administrative**
  - Examples: separation of duties, dual control, etc

- **Physical**
  - Examples: fences, alarms, badges, CCTV, etc

- **Technical**
  - Examples: antivirus, antis-spam, logs, etc
Metode Access Control

- Administrative Controls
  - Policy and Procedure
  - Personnel Controls
    - Separation of Duties
    - Rotation of Duties
    - Mandatory Vacation
  - Supervisory Structure
  - Security Awareness Training
  - Testing
Metode Access Control

- **Physical Controls**
  - Network Segregation
  - Perimeter Security
  - Computer Controls
  - Work Area Separation
  - Data Backups
  - Cabling
  - Control Zone
Metode Access Control

- **Technical (Logical) Controls**
  - System Access
  - Network Architecture
  - Network Access
  - Encryption and protocols
  - Auditing
Each control works at a different level of granularity, but can also perform several functions.

Access Control Functionalities
- Prevent
- Detect
- Correct
- Deter
- Recover
- Compensate
Tipe-tipe Access Control

- Preventive Access controls
  - Avoid having unwanted actions/events by blocking the ability to do them.

- Detective
  - Identify unwanted actions or events after they occur.

- Corrective
  - Remedy circumstances that enabled the unwanted activity.
  - Return to state prior to the unwanted activity.

- Directive
  - Dictated by higher authority in laws or regulations or those specified in organization policy

- Deterrent
  - Prescribe punishment for noncompliance

- Recovery
  - Restore lost computing resources or capabilities.

- Compensating
  - Reinforce or replace normal controls that are unavailable.
Preventive Controls

- Block or control specific events
  - Firewalls
  - Anti-virus software
  - Encryption
  - Key card systems
  - Bollards stop cars (as shown)
Tipe-tipe Access Control

- **Deterrent Controls**
  - Highly visible
  - Prevent offenses by influencing choices of would-be intruders

- **Detective Controls**
  - Monitor and record specific types of events
  - Does not stop or directly influence events
Corrective Controls
- Post-event controls to prevent recurrence
- “Corrective” refers to *when* it is implemented
- Examples (if implemented after an incident)
  - Spam filter
  - Anti-virus on e-mail server
  - WPA Wi-Fi encryption

Recovery Control
- Post-incident controls to recover systems
Compensating Controls

- Control that is introduced that compensates for the absence or failure of a control

- “Compensating” refers to why it is implemented

Examples

- Daily monitoring of anti-virus console
- Monthly review of administrative logins
- Web Application Firewall used to protect buggy application
Hubungan Metode dan Tipe Access Control

<table>
<thead>
<tr>
<th>Controls</th>
<th>Administrative</th>
<th>Technical</th>
<th>Physical</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Directive</strong></td>
<td>Policy</td>
<td>Warning Banner</td>
<td>‘Do Not Enter’</td>
</tr>
<tr>
<td><strong>Deterrent</strong></td>
<td>Demotion</td>
<td>Violation Reports</td>
<td>‘Beware of Dog’</td>
</tr>
<tr>
<td><strong>Preventive</strong></td>
<td>User Registration</td>
<td>Passwords, Tokens</td>
<td>Fences, Bollards</td>
</tr>
<tr>
<td><strong>Detective</strong></td>
<td>Report Reviews</td>
<td>Audit Logs, IDS</td>
<td>Sensors, CCTV</td>
</tr>
<tr>
<td><strong>Corrective</strong></td>
<td>Employee Termination</td>
<td>Connection Management</td>
<td>Fire Extinguisher</td>
</tr>
<tr>
<td><strong>Recovery</strong></td>
<td>DRP</td>
<td>Backups</td>
<td>Reconstruct, Rebuild</td>
</tr>
<tr>
<td><strong>Compensating</strong></td>
<td>Supervision, Job Rotation</td>
<td>Keystroke Logging</td>
<td>Layered Defenses</td>
</tr>
</tbody>
</table>
Akuntabilitas

- Accountability is tracked by recording user, system, and application activities.

- Audit information must be reviewed
  - Event Oriented Audit Review
  - Real Time and Near Real Time Review
  - Audit Reduction Tools
  - Variance Detection Tools
  - Attack Signature Tools
Other accountability concepts...

Keystroke Monitoring
- Can review and record keystroke entries by a user during an active session.
- A hacker can also do this
- May have privacy implications for an organization

Scrubbing: Removing specific incriminating data within audit logs
Penerapan Access Control

- Know the access control tasks that need to be accomplished regularly to ensure satisfactory security. Best practices include:
  - Deny access to anonymous accounts
  - Enforce strict access criteria
  - Suspend inactive accounts
  - Replace default passwords
  - Enforce password rotation
  - Audit and review
  - Protect audit logs
Penerapan Access Control

- Unauthorized Disclosure of Information
  - Object Reuse
  - Data Hiding

- Emanation Security (Security to block electrical signals from electronic equipment.)
  - **Tempest**: a project started by the DoD and then turned into a standard that outlines how to develop countermeasures that control spurious electrical signals that are emitted by electronic equipment.
  - **White Noise**: A uniform spectrum of random electrical signals. It is distributed over the full spectrum so that the bandwidth is constant and an intruder is not able to decipher real information from random noise or random information.
  - **Control Zone**: Creates a security perimeter and is constructed to protect against unauthorized access to data or compromise of sensitive information.
Testing Access Controls

- Access controls are the primary defense that protect assets

- Types of tests:
  - Penetration tests
  - Application vulnerability tests
  - Code reviews

http://secunia.com/community/
Penetration Testing

- Automatic scans to discover vulnerabilities

- Example tools: Nessus, Nikto, SAINT, Superscan, Retina, ISS, Microsoft Baseline Security Analyzer
Application Vulnerability Testing

- Discover vulnerabilities in an application

- Automated tools and manual tools

- Example vulnerabilities
  - Cross-site scripting, injection flaws, malicious file execution, broken authentication, broken session management, information leakage, insecure use of encryption, and many more
Testing Access Controls

Audit Log Analysis

 Regular examination of audit and event logs
 Detect unwanted events
  • Audit log protection
Monitoring Access Control

- Intrusion Detection
  - Three Common Components
    » Sensors
    » Analyzers
    » Administrator Interfaces
  - Common Types
    » Intrusion Detection
    » Intrusion Prevention
    » Honeypots
    » Network Sniffers
Monitoring Access Control

- Two Main Types of Intrusion Detection Systems
  - Network Based (NIDS)
  - Host Based (HIDS)

- HIDS and NIDS can be:
  - Signature Based
  - Statistical Anomaly Based
    - Protocol Anomaly Based
    - Traffic Anomaly Based
  - Rule Based
Monitoring Access Control

- Intrusion Prevention Systems
  - The next big thing
  - Is a preventative and proactive technology, IDS is a detective technology.
  - Two types: Network Based (NIPS) and Host Based (HIPS)
Monitoring Access Control

- **Honeypots**
  - An attractive offering that hopes to lure attackers away from critical systems

- **Network sniffers**
  - A general term for programs or devices that are able to examine traffic on a LAN segment.
A few threats to access control

- Insiders
  - Countermeasures include good policies and procedures, separation of duties, job rotation
- Dictionary Attacks
  - Countermeasures include strong password policies, strong authentication, intrusion detection and prevention
- Brute Force Attacks
  - Countermeasures include penetration testing, minimum necessary information provided, monitoring, intrusion detection, clipping levels
- Spoofing at Logon
  - Countermeasures include a guaranteed trusted path, security awareness to be aware of phishing scams, SSL connection
Serangan pada Access Control

- Intruders will try to defeat, bypass, or trick access controls in order to reach their target

- Attack objectives
  - Guess credentials
  - Malfunction of access controls
  - Bypass access controls
  - Replay known good logins
  - Trick people into giving up credentials
Buffer Overflow

- Cause malfunction in a way that permits illicit access
- Send more data than application was designed to handle properly
- **Countermeasure**: “safe” coding that limits length of input data; filter input data to remove unsafe characters
Script Injection

- Insertion of scripting language characters into application input fields
  - Execute script on server side
  - Execute script on client side – trick user or browser
- **Countermeasures**: strip “unsafe” characters from input
Data Remanence

- Literally: data that remains after it has been “deleted”

- Examples
  - Deleted hard drive files
  - Erased files
  - Discarded / lost media: USB keys, backup tapes, CDs
Denial of Service (DoS)

- Actions that cause target system to fail, thereby *denying service* to legitimate users
  - Distributed Denial of Service (DDoS)

- **Countermeasures**: input filters, patches, high capacity
Eavesdropping

- Interception of data transmissions
- **Countermeasures**: encryption, stronger encryption
Spoofing and Masquerading

- Specially crafted network packets that contain forged address of origin

- **Countermeasures**: router / firewall configuration to drop forged packets, judicious use of e-mail for signaling or data transfer

http://www.techrepublic.com/blog/security/how-to-spoof-a-mac-address/395
Social Engineering

- Tricking people into giving out sensitive information by making them think they are *helping* someone
- Countermeasures: security awareness training
Phishing

- Incoming, fraudulent e-mail messages designed to give the appearance of origin from a legitimate institution
- Tricks user into providing sensitive data via a forged web site (common) or return e-mail (less common)
Pharming

- Redirection of traffic to a forged website
- **Countermeasures**: user awareness training, patches, better controls
Serangan pada Access Control

Malicious Code

- Viruses, worms, Trojan horses, spyware, key logger
- Harvest data or cause system malfunction
- Countermeasures: anti-virus, anti-spyware, security awareness training
Model Arsitektur Keamanan untuk AC

• Can help organizations quickly make improvements through adaptation

• Can focus on:
  – computer hardware and software
  – policies and practices
  – the confidentiality of information
  – the integrity of the information
  – **Pick one and go with it**
Bell-LaPadula Confidentiality Model

- A state machine model that helps ensure the confidentiality of an information system
  - Using mandatory access controls (MACs), data classification, and security clearances
Biba Integrity Model

• Provides access controls to ensure that objects or subjects cannot have less integrity as a result of read/write operations

• Ensures no information from a subject can be passed on to an object in a higher security level
  – This prevents contaminating data of higher integrity with data of lower integrity
Clark-Wilson Integrity Model

• Built upon principles of change control rather than integrity levels

• Its change control principles
  – No changes by unauthorized subjects
  – No unauthorized changes by authorized subjects
  – The maintenance of internal and external consistency
Model Arsitektur Keamanan untuk AC

Graham-Denning Access Control Model

• Composed of three parts
  – A set of objects
  – A set of subjects (a process and a domain)
  – A set of rights

• Primitive protection rights
  – Create or delete object, create or delete subject
  – Read, grant, transfer and delete access rights
Harrison-Ruzzo-Ullman Model

- Defines a method to allow changes to access rights and the addition and removal of subjects and objects
  - Since systems change over time, their protective states need to change
- Built on an access control matrix
- Includes a set of generic rights and a specific set of commands
Brewer-Nash Model (aka Chinese Wall)

- Designed to prevent a conflict of interest between two parties
- Requires users to select one of two conflicting sets of data, after which they cannot access the conflicting data
The ISO 27000 Series

• Information Technology – Code of Practice for Information Security Management
  – One of the most widely referenced and discussed security models
  – Originally published as British Standard 7799 and then later as ISO/IEC 17799
  – Since been renamed ISO/IEC 27002

• Establishes guidelines for initiating, implementing, maintaining, and improving information security management
## Model Arsitektur Keamanan untuk AC

(Lanjutan)

<table>
<thead>
<tr>
<th>ISO 27000 Series Standard</th>
<th>Status</th>
<th>Title or Topic</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>27000</td>
<td>May 2009</td>
<td>Series Overview and Terminology</td>
<td>Defines terminology and vocabulary for the standard series</td>
</tr>
<tr>
<td>27001</td>
<td>2005</td>
<td>Information Security Management System Specification</td>
<td>Drawn from BS 7799:2</td>
</tr>
<tr>
<td>27002</td>
<td>July 2007</td>
<td>Code of Practice for Information Security Management</td>
<td>Renamed from ISO/IEC 17799, drawn from BS 7799:1</td>
</tr>
<tr>
<td>27003</td>
<td>Planned</td>
<td>Information Security Management Systems Implementation Guidelines</td>
<td>Expected late 2009 or 2010</td>
</tr>
<tr>
<td>27004</td>
<td>Planned</td>
<td>Information Security Measurements and Metrics</td>
<td>Expected in late 2009 or 2010</td>
</tr>
<tr>
<td>27005</td>
<td>2008</td>
<td>ISMS Risk Management</td>
<td></td>
</tr>
<tr>
<td>27006</td>
<td>2007</td>
<td>Requirements for Bodies Providing Audit and Certification of an ISMS</td>
<td>Is largely intended to support the accreditation of certification bodies providing ISMS certification</td>
</tr>
<tr>
<td>27007</td>
<td>Planned</td>
<td>Guidelines for ISMS Auditing</td>
<td>Focuses on management systems</td>
</tr>
<tr>
<td>27008</td>
<td>Planned</td>
<td>Guidelines for ISMS Auditing</td>
<td>Focuses on security controls</td>
</tr>
<tr>
<td>27011</td>
<td>2008</td>
<td>Information Security Guidelines for the Telecommunications Industry</td>
<td></td>
</tr>
<tr>
<td>27014</td>
<td>Planned</td>
<td>Information Security Governance Framework</td>
<td></td>
</tr>
<tr>
<td>27015</td>
<td>Planned</td>
<td>Information Security Management Guidelines for the Finance and Insurance Sectors</td>
<td></td>
</tr>
<tr>
<td>27032</td>
<td>Planned</td>
<td>Guideline for Cybersecurity</td>
<td></td>
</tr>
<tr>
<td>27034</td>
<td>Planned</td>
<td>Guideline for Application Security</td>
<td></td>
</tr>
</tbody>
</table>
Model Arsitektur Keamanan untuk AC

Control Objectives for Information and Related Technology (COBIT)

• Control Objectives for Information and Related Technology (COBIT)
  – Provides advice about the implementation of sound controls and control objectives for InfoSec
  – Created by the Information Systems Audit and Control Association (ISACA) and the IT Governance Institute (ITGI) in 1992
COSO

• U.S. private-sector initiative
  – Major Objective: identify factors that cause fraudulent financial reporting and to make recommendations to reduce its incidence
  – Has established a common definition of internal controls, standards and criteria
  – Helps organizations comply with critical regulations like Sarbanes-Oxley
COSO (Lanjutan)

- Built on five interrelated components:
  - Control environment
  - Risk assessment
  - Control activities
  - Information and communication
  - Monitoring
- Selesai -