



# **Australian Standard 8015 : 2005**

Arrianto Mukti Wibowo, M.Sc., CISA

IT Governance Lab  
Faculty of Computer Science  
University of Indonesia

**CORPORATE  
GOVERNANCE OF  
INFORMATION &  
COMMUNICATION  
TECHNOLOGY**



# Agenda

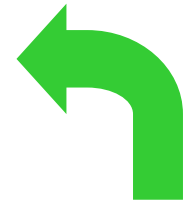
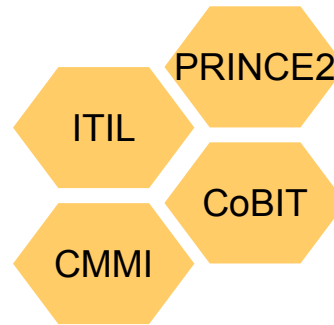
- Intro, Tujuan, definisi,
- Prinsip-prinsip
- Model AS-8015

# Keluarga Besar dari AS-8015

- The 8000 series of Corporate Governance standards published in 2004 provide guidance for those wishing to do better.
  - Good Governance Principles (AS8000)
  - Fraud and Corruption Control (AS8001)
  - organisational Codes of Conduct (AS8002)
  - Corporate Social Responsibility (AS8003)
  - Whistle Blower protection programs (AS8004)
  - GCG for ICT (AS8015)
- The widely acknowledged AS4360 Risk Management standard was also revised in 2004.
- This along with the adoption of BS15000 (now ISO 20000) as AS8018 IT Service Management, provided the context for the drafting and subsequent publishing of AS8015 to provide guidance on the small "c", corporate governance of Information and Communication Technology.

# Reasons for AS-8015

- IT is mostly doing its internal job competently:
  - Rigour
  - Process
  - Reporting
  - Control
- But business leaders are **STILL** not engaging with IT:
  - Not responsible
  - Not setting direction
  - Not planning
  - Not implementing



Improving  
Supply

...

...

does  
not fix  
demand!



# Tujuan Adanya AS-8015

1. To provide a framework of principles for Directors to use when evaluating, directing and monitoring the information and communication technology (ICT) portfolio in their organizations.
2. To promote effective, efficient, and acceptable use of ICT in all organizations by—
  - (a) providing stakeholders (including consumers, shareholders, and employees) with the confidence that, if the Standard is followed, they can trust in the organization's corporate governance of ICT;
  - (b) informing and guiding Directors in governing the use of ICT in their organization; and
  - (c) providing a basis for objective evaluation of the corporate governance of ICT.

# Australian Standard-8015

## Good Corporate Governance for ICT

*“The system by which the current and future use of ICT is directed and controlled. It involves evaluating and directing the plans for the use of ICT to support the organisation and monitoring this use to achieve plans. It includes the strategy and policies for using ICT within an organisation.”*

# Who are the directors?

- Member of the most senior governing body of an organization.
- Includes owners, board members, Directors, partners, senior executives or similar, and officers authorized by Acts of Parliament *(mungkin maksudnya para petinggi yang namanya harus ada dalam statuta perusahaan menurut undang-undang tertentu)*





# **Principles of GCG for ICT**

# The 6 Principles

1. Establish clearly understood responsibilities for ICT
2. Plan ICT to best support the organization
3. Acquire ICT validly
4. Ensure that ICT performs well, whenever required
5. Ensure ICT conforms with formal rules
6. Ensure ICT use respects human factors

## **Principle 1:**

# **Establish clearly understood responsibilities for ICT**

- Ensure that individuals and groups within the organization understand and accept their responsibilities for ICT.

## **Principle 2 :**

# **Plan ICT to best support the organization**

- Ensure that ICT plans fit the current and ongoing needs of the organization and that the ICT plans support the corporate plans

# Principle 3:

## Acquire ICT validly

- Ensure that ICT acquisitions are made for approved reasons in the approved way; on the basis of appropriate and ongoing analysis.
- Ensure that there is appropriate balance between costs, risks, long term and short term benefits.

## **Principle 4:**

### **Ensure that ICT performs well, whenever required**

- Ensure that ICT is fit for its purpose in supporting the organization, is kept responsive to changing business requirements, and provides support to the business at all times when required by the business.

# **Principle 5:**

## **Ensure ICT conforms with formal rules**

- Ensure that ICT conforms with all external regulations and complies with all internal policies and practices.

# **Principle 6:**

## **Ensure ICT use respects human factors**

- Ensure that ICT meets the current and evolving needs of all the 'people in the process'.



# AS-8015 Model

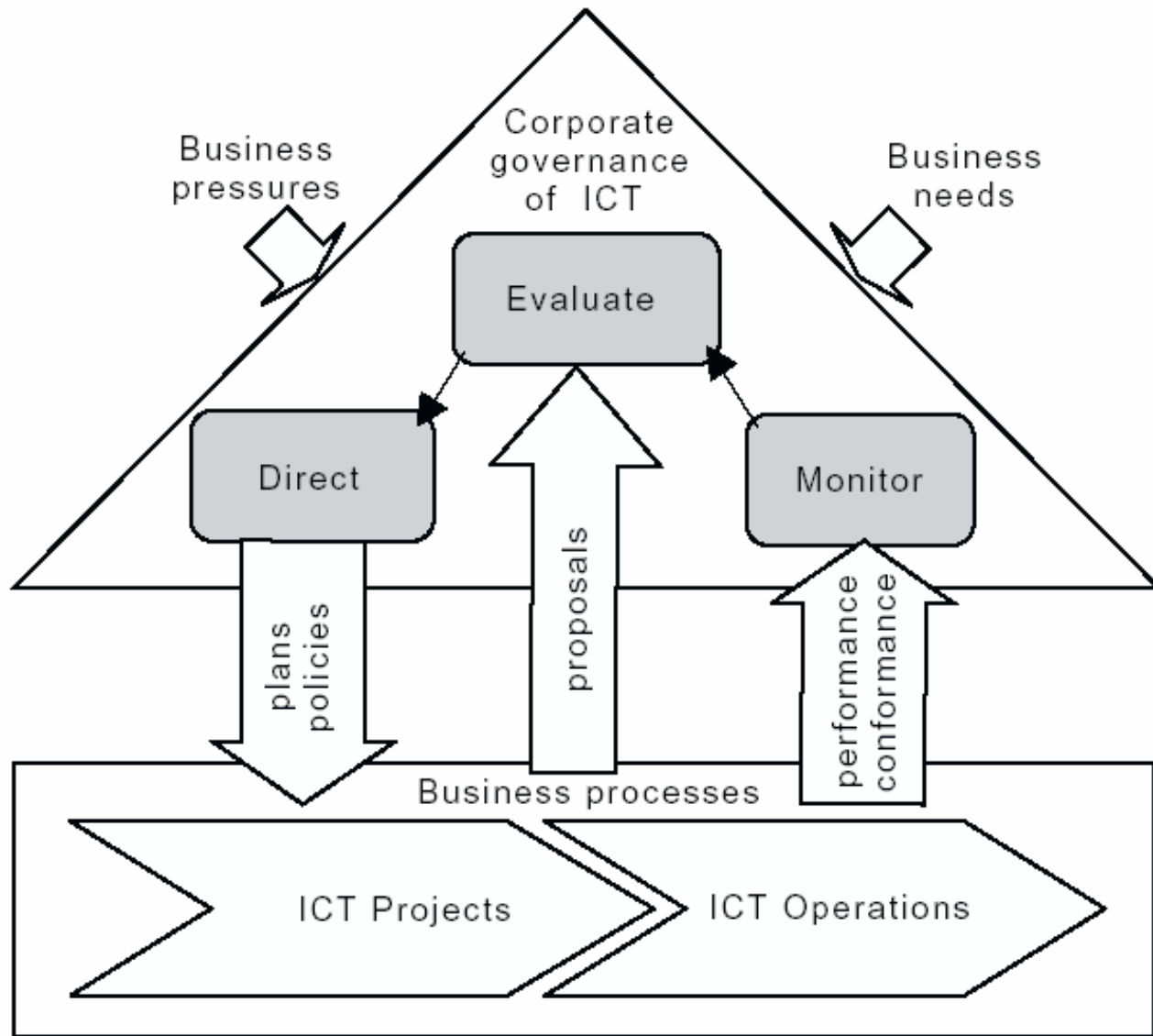


# Three main task of directors

1. Evaluate the use of ICT
2. Direct preparation and implementation of plans and policies.
3. Monitor conformance to policies, and performance against the plans.

*Responsibility for specific aspects of ICT' may be delegated. However, the accountability for the effective, efficient and acceptable use of ICT by an organization, remains with its Directors*

# AS-8015 Model



# Evaluation of ICT

- In evaluating the use of ICT, directors should consider the pressures acting upon the business. Such as technological change, economic and social trends, and political influences.
- Directors should also take account of the business needs the organizational objectives that they must achieve, such as maintaining competitive advantages.

# Direct Plan & Implementation ICT

- Directors should direct the preparation and implementation of plans and policies and assign responsibilities for this implementation.
- Plans should set the direction for investments in ICT projects or changes in ICT operations.
- Policies should establish sound behaviour in the use of ICT.
- Directors should ensure that the transition from projects to operations takes into account impacts on operational practices and existing ICT infrastructure.  
*Jadi bukan sekedar “IT Project” tetapi sustain sampai ke pelaksanaan sehari-hari pasca proyek...!*

# Monitor ICT

- To complete the cycle the directors should monitor through appropriate performance measurement system the performance of the ICT.
- They should reassure themselves that *performance is in accordance with plans*.
  - Jadi mengaudit TI bukan sekedar asal audit...!
- They should also make sure that the use of ICT conforms with external legal obligations and internal work practices.
- If necessary they should direct the submission of proposals for approval to address identified needs.

# ICT Governance Framework

The following table lists the general principles of sound ICT governance and the actions required by Directors to implement the principles.

They are applicable to most organizations most of the time and any variation should be well considered.



# ICT Governance Principles (1-2)

Ref No.	Principle	Actions to Implement the Principles		
		Evaluate	Direct	Monitor
1	Establish clearly understood responsibilities for ICT	<p>Directors should evaluate the options for assigning the responsibilities for the effective, efficient, and acceptable use of ICT.</p> <p>Directors should ensure that those given responsibility are competent. Generally these will be <b>business managers</b> assisted by ICT specialists who understand business values and processes.</p> <p>Directors should evaluate developments in ICT and business processes to ensure that ICT will provide support for future business needs.</p>	<p>Directors should direct that plans are carried out and policies implemented according to the assigned ICT responsibilities.</p>	<p><b>Directors retain ultimate responsibility</b> for the execution of the plans and proposals. They should satisfy themselves that appropriate ICT governance mechanisms are established.</p> <p>Directors should monitor the performance of those given responsibility in the governance of ICT (for example, in serving on steering committees or in presenting proposals to Directors).</p> <p>Directors should ensure that <b>they receive the information that they need to meet their responsibilities by establishing and appropriately reviewing measurement systems.</b></p>
2	Plan ICT to best support the organization	<p>In formulating plans and policies Directors should evaluate ICT activities to ensure they align with the organization's objectives for changing circumstances, consider better practices and satisfy other key stakeholder requirements.</p> <p>Directors should use prudent risk management procedures as described in AS/NZS 4360.</p>	<p>Directors should direct that proposals are submitted for <b>approval in a timely fashion</b> to address gaps identified in the evaluation of ICT activities.</p> <p>Directors should also encourage the submission of proposals for <b>innovative uses of ICT that enable the organization to undertake new businesses or improve processes.</b></p> <p>Directors should direct the preparation and use of plans and policies that ensure the organization benefits from developments in ICT.</p>	<p>Directors should monitor the progress of approved ICT proposals to ensure that they are achieving objectives in required time frames using allocated resources.</p> <p>Directors should monitor the use of ICT to ensure that it is achieving its intended benefits.</p>



# ICT Governance Principles (3-4)

Ref No.	Principle	Actions to Implement the Principles		
		Evaluate	Direct	Monitor
3.	Acquire ICT validity	<p>Directors should monitor the progress of approved ICT proposals to ensure that they are <b>achieving objectives in required time frames using allocated resources</b>.</p> <p>Directors should monitor the use of ICT to ensure that it is achieving its <b>intended benefits</b>.</p>	<p>Directors should direct that ICT assets (systems and infrastructure) are <b>acquired</b> in an appropriate manner, including the preparation of suitable documentation, while ensuring that required capabilities are provided.</p> <p>Directors should direct that their organization and suppliers develop a <b>shared understanding of the organization's intent</b> in making any ICT acquisition.</p>	<p>Directors should monitor ICT acquisitions to ensure that they do provide the required capabilities.</p> <p>Directors should monitor the extent to which their organization and suppliers maintain the shared understanding of the organization's intent in making any ICT acquisition.</p>
4.	Ensure ICT performs well, whenever required	<p>Directors should evaluate the risks to the integrity of information and the protection of ICT assets from damage, abuse, or misuse.</p> <p>Directors should evaluate options to ensure that ICT will support business processes with the required capability and capacity.</p>	<p>Directors should direct those responsible to ensure that ICT supports the business when required for business reasons, with correct and up-to-date data while protected from loss or misuse, in accordance with <b>AS/NZS ISO/IEC 17799 and AS/NZS 7799.2</b>.</p> <p>Directors should direct that <b>resources be allocated sufficiently</b> to ensure that ICT meets the needs of the organization according to the priorities that they have set.</p>	<p>Directors should monitor the extent to which ICT does support the business.</p> <p>Directors should monitor ICT to ensure that assets are decommissioned and disposed of in accordance with environmental and data management requirements.</p> <p>Directors should <b>monitor the extent to which the policies for data accuracy</b> and the efficient use of ICT are followed properly.</p>

# ICT Governance Principles (5-6)

Ref No.	Principle	Actions to Implement the Principles		
		Evaluate	Direct	Monitor
5.	Ensure ICT conforms with formal rules	Directors should regularly evaluate the extent to which ICT satisfies internal obligations including legislation, internal policies, standards and professional guidelines.	Directors should <b>direct those responsible to establish regular and routine mechanisms for ensuring that the use of ICT complies</b> with relevant legislation. Directors should direct that policies are established and enforced to enable the organization to meet its internal obligations in its use of ICT. Directors should direct that ICT staff follow the guidelines set by their professions. Directors should direct that all actions relating to ICT be ethical.	Directors should monitor the manner in which managers are reviewing ICT compliance and conformance to ensure that the reviews are <b>timely</b> , comprehensive, and suitable for the evaluation of the extent of satisfaction of internal obligations.
6.	Ensure ICT use respects human factors	Directors should evaluate ICT activities to ensure that <b>people's concerns are appropriately considered</b> and their <b>needs identified</b> .	Directors should direct that ICT activities are consistent with identified needs. Directors should direct that <b>risks may be raised by anyone at any time</b> . They should be managed in accordance with published policies and procedures and <b>escalated</b> to the relevant decision makers.	Directors should monitor ICT activities to ensure that identified needs remain relevant. Directors should monitor work practices to ensure that they are consistent with the appropriate use of ICT.