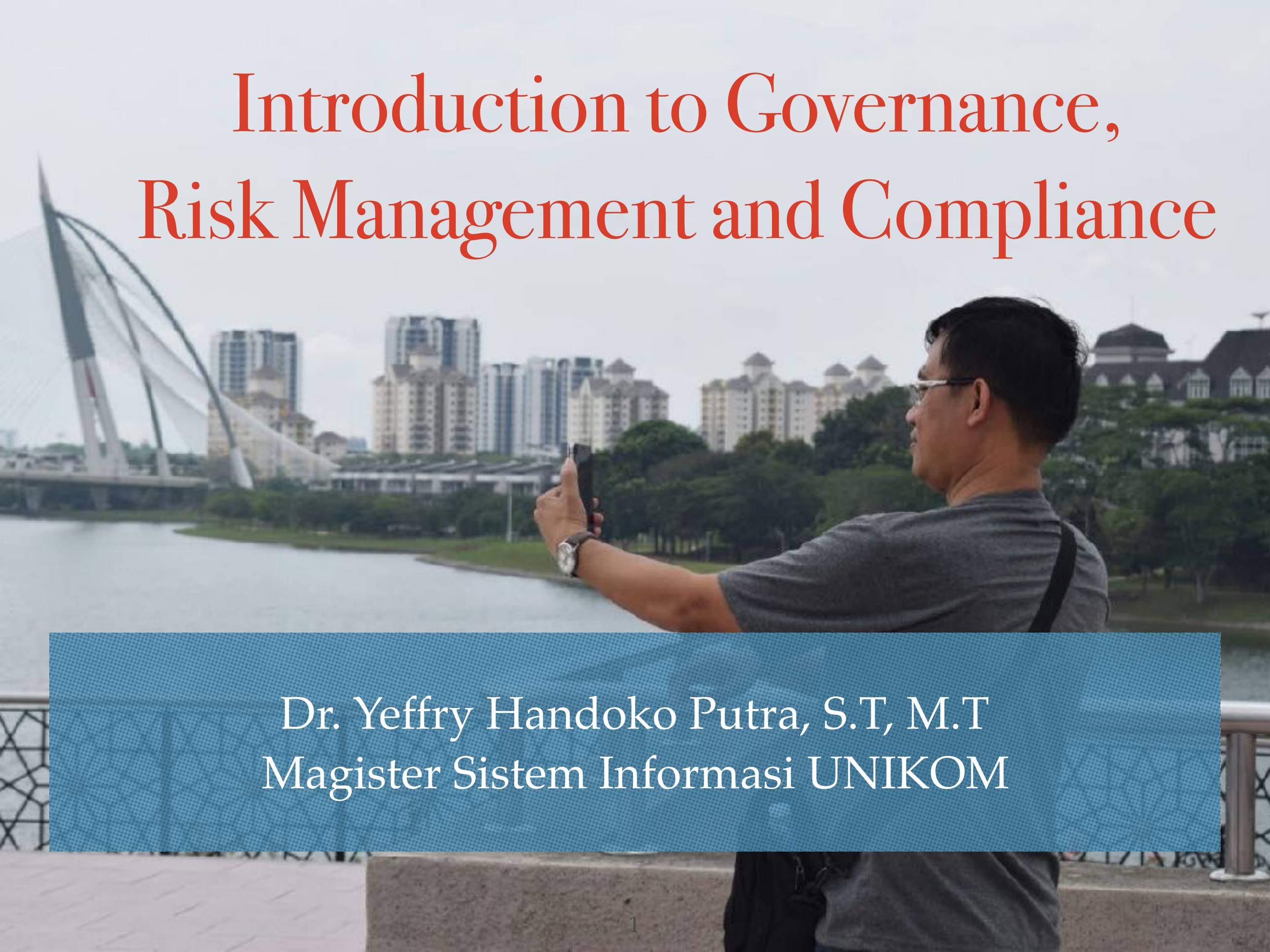
Introduction to Governance, Risk Management and Compliance



Dr. Yeffry Handoko Putra, S.T, M.T
Magister Sistem Informasi UNIKOM

Governance, Risk & Compliance...

- **Governance -** setting business strategy & objectives, determining risk appetite, establishing culture & values, developing internal policies and monitoring performance.

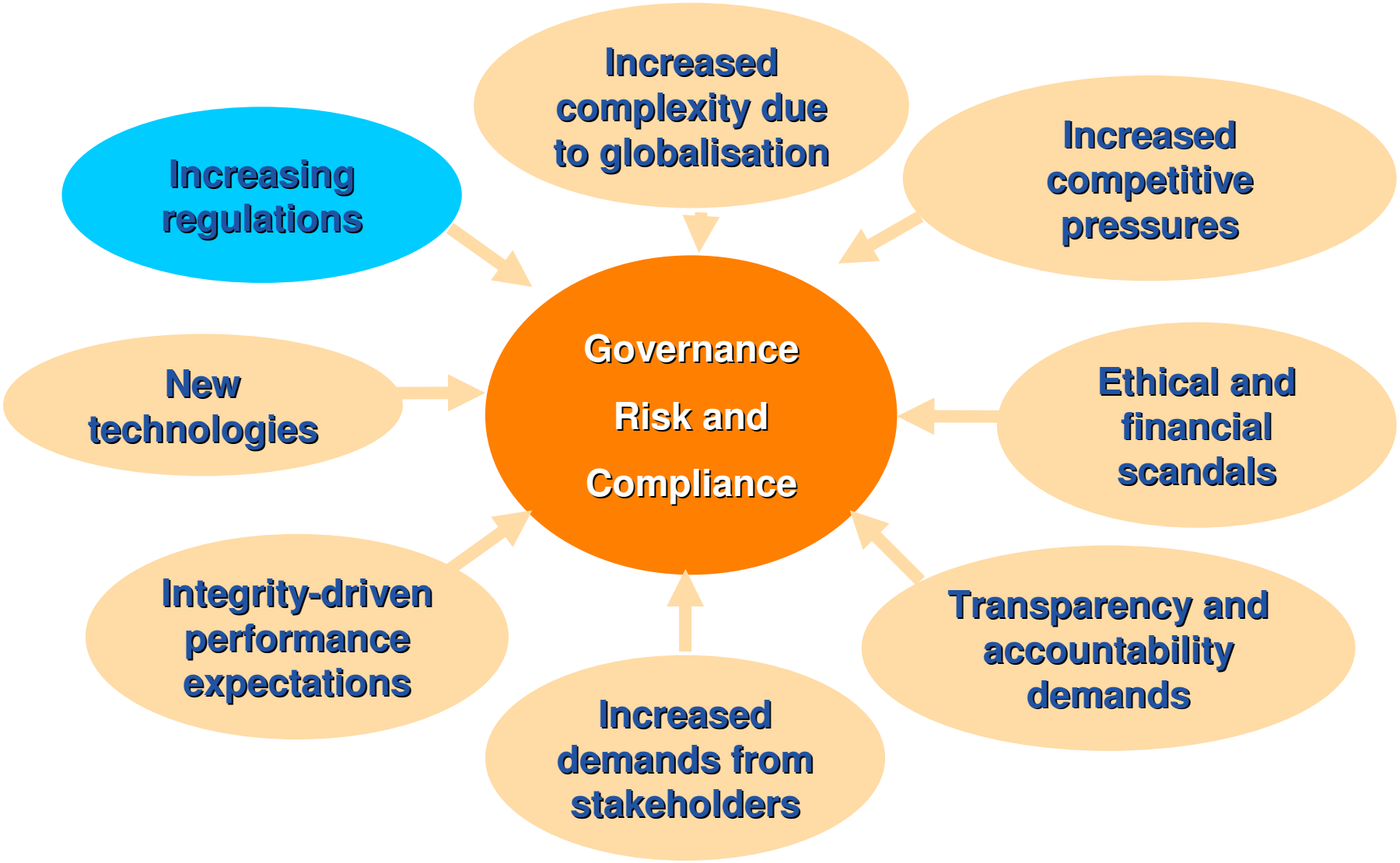
- **Risk Management -** identifying and assessing risk that may affect the ability to achieve objectives, applying risk management to gain competitive advantage and determine risk response strategies and control activities.

- **Compliance -** operating in accordance with objectives and ensuring adherence with laws and regulations, internal policies & procedures, and stakeholder commitments.

Governance, Risk & Compliance...

GRC provides a framework and a methodology to enable those responsible for managing the business to give confidence to those who are accountable to shareholders and to regulators that corporate objectives are being met.

Business drivers for an integrated approach to Governance, Risk and Compliance



Risk

- 风险

In simplified Chinese the word risk is composed by two characters; one represents danger, and the other represents opportunity.

Definition of Risk

- "Risk is a measure of future uncertainties in achieving program performance goals and objectives within defined cost, schedule, and performance constraints."*[1]*
- "...an uncertain event or condition that, if it occurs, has a positive or negative effect on a project objective." *[2]*

[1] *Risk Management Guide for DoD Acquisition*, Sixth Edition DoD, DAU, August 2006

[2] *Project Management Institute PMBOK®*, 2008, Fourth Edition

Likelihood of an event occurring. The consequence if such an event occurs.

Enterprise Risk and Compliance-Drivers and Trends

- **Drivers:**
  - Multiplicity of risk and regulations
  - Distributed operations and relationships
  - Interdependency of risk
  - Increased accountability
  - Fragmentation and duplication of effort
- **2009 – 2010 trends:**
  - Establishment of risk and compliance architecture
  - Development of risk intelligence
  - Implementation of GRC platforms
  - Centralized communication and training on corporate policies and procedures
  - Continued evolution of the CxO responsible for GRC

Risk Sensors

Risk Sensors can provide automated inputs from low level data;

- to demonstrate compliance to legislation and regulation (and non-compliance)
- to demonstrate working controls (and not working controls)
- to highlight risks / threats
- to identify incidents
- to highlight possible data leakage
- identify potential reputation damage

+ many more……

Example of Sensors

Sensors to detect events

- System monitors
  - Vulnerability assessment, configuration and policy compliance
- Network traffic monitors
  - Intrusion detection, Intrusion prevention, Firewalls, Routers,
- Access and identity monitors
  - Failed logins, privilege escalation, Bio-metric identities
- Web site monitors
  - Pages visited, referred from,
- End point monitoring
  - Data leakage
  - Anti-virus, anti-phishing, Malware detection
- Others
  - Event and Audit log collection – OS, Infrastructure, applications
  - CMDB systems
  - Incident management
  - Backup software, Business continuity management
  - IT Security Information (intelligence feeds)
- Emerging
  - Virtualised environments / 'Cloud' computing

Thank You