

CYBERSECURITY GOVERNANCE, RISK AND STANDARD

SARWONO SUTIKNO, DR.ENG., CISA, CISSP, CISM

KEYNOTE SPEECH - MICEEI 2014 - MAKASAR 26-30 NOV 20141



SARWONO SUTIKNO, DR.ENG., CISA, CISSP, CISM

Current:

- Cybersecurity Nexus Liaison ISACA Indonesia
- ISACA Academic Advocate at ITB
- SME for Information Security Standard for ISO at ISACA HQ
- Associate Professor at School of Electrical Engineering and Informatics, Institut Teknologi Bandung
- Ketua WG Layanan dan Tata Kelola TI, anggota WG Keamanan Informasi serta Anggota Panitia Teknis 35-01 Program Nasional Penetapan Standar bidang Teknologi Informasi, BSN Kominfo.

Past:

- Director of Certification CRISC & CGEIT, ISACA Indonesia Chapter
- Ketua Kelompok Kerja Evaluasi TIK Nasional, Dewan TIK Nasional (2007-2008)
- Plt Direktur Operasi Sistem PPATK (Indonesia Financial Transaction Reports and Analysis Center, INTRAC), April 2009 May 2011

Professional Certification:

- Professional Engineering (PE), the Principles and Practice of Electrical Engineering, College of Engineering, the University of Texas at Austin. 2000
- IRCA Information Security Management System Lead Auditor Course, 2004
- ISACA Certified Information System Auditor (CISA). CISA Number: 0540859, 2005
- Brainbench Computer Forensic, 2006
- (ISC)² Certified Information Systems Security Professional (CISSP), No: 118113, 2007
- ISACA Certified Information Security Manager (CISM). CISM Number: 0707414, 2007

Award:

 (ISC)² Asia Pacific Information Security Leadership Achievements (ISLA) 2011 award in category Senior Information Security Professional. http://isc2.org/ISLA

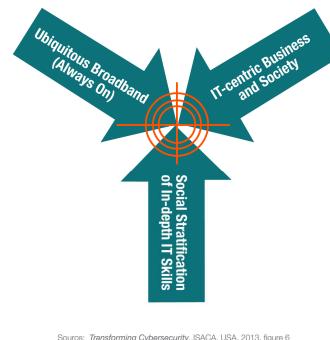




CYBERSECURITY - INFORMATION SECURITY

Cybersecurity is emerging within the fields of information security and traditional security to address sharp increases in cybercrime and, in some instances, evidence of cyberwarfare.

Cybersecurity includes the protection of information assets by addressing threats to information that is processed, stored and transported by internetworked information systems.

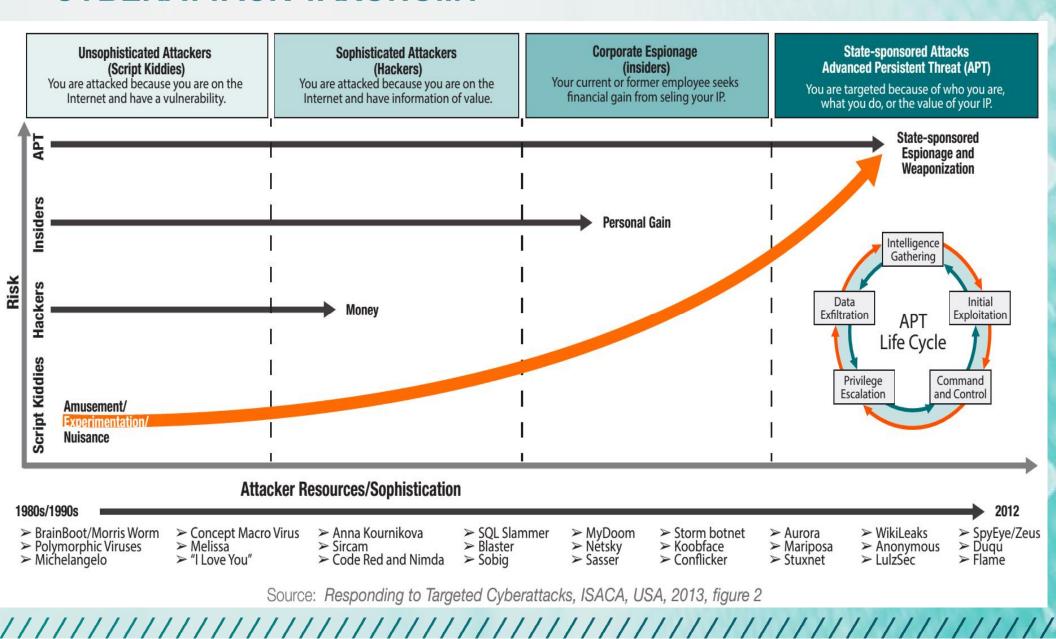


Source: Transforming Cybersecurity, ISACA, USA, 2013, figure 6





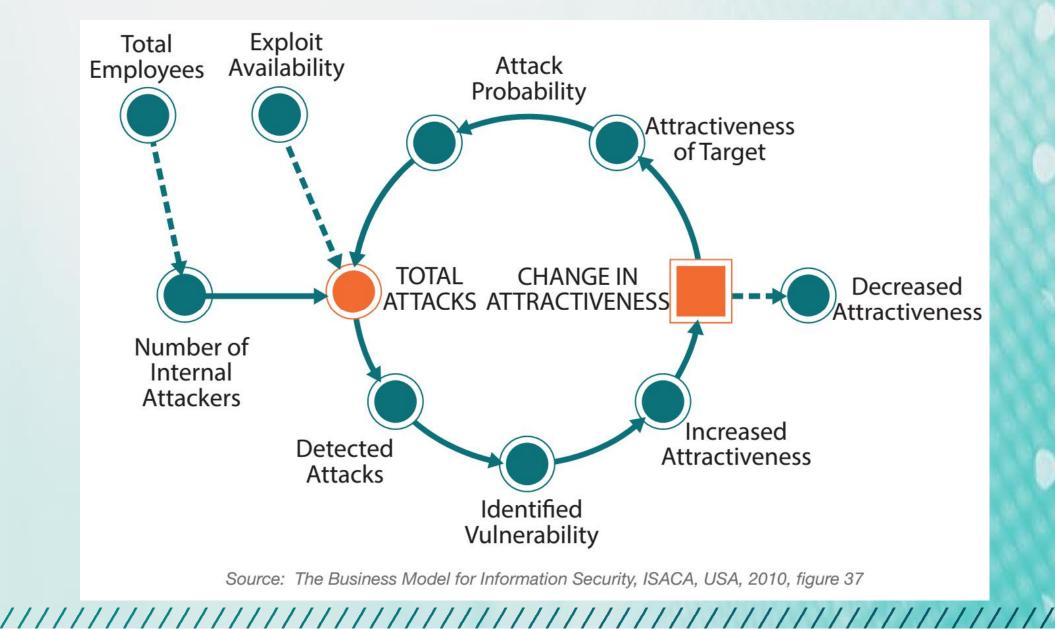
CYBERATTACK TAXONOMY







CYBERSECURITY SYSTEM DYNAMICS







ASSURANCE – THREE LINES OF DEFENCE

- Internal controls testing
- Cybersecurity compliance
- Formal risk acceptances
- Investigation/forensics

- Threats, vulnerailities, risk
- Formal risk evaluation
- Business impact analysis (BIA)
- Emerging risk

- Control self-assessments (CSAs)
- Attack/breach penetration testing
- Functional/technical testing
- Social/behavioral testing
- Regular management review

Third line—Internal Audit



Second line—Risk Management



First line—Management

Source: Transforming Cybersecurity, ISACA, USA, 2013, figure 45





RISK BASED CATEGORIZATION OF CONTROL

Organizational Controls

- Design and structure
- Compliance and control
- Culture (organizational)

Social Controls

- People
- Culture (individual)
- Human factors
- Emergence

Technical Controls

- Architecture
- Apps/operating systems
- Infrastructure
- Technical infrastructure

Process Controls

- Technical processes
- Man-machine interfaces
- Infrastructural life cycle
- · Etc.





ORGANIZATION LAYER CONTROL

Design and Structure

- Cybersecurity unit
- Links to crisis/incident management teams
- Internal CERTs
- Forensics unit
- Embedded external experts
- Links to external agencies

Organizational Culture

- Defined tolerance levels
- Ongoing awareness campaign
- Model behaviors
- Whistle-blowing channels

- Help line/help desk
- Opt-in surveillance
- Intelligence gathering

Compliance

- Policies, standards, procedures
- · Monitoring and reporting
- Rules of enforcement
- Forensics
- Internal and external audit
- Incident handling rules
- Etc.





SOCIAL LAYER CONTROL

People

- Model behaviors
- Skills and training
- Integrity checks
- Individual use controls
- Social networking controls
- Traveling/home use controls
- Family contextual controls

Individual Culture

- Defined trust levels
- Attitudes toward IT use
- Regional/national context and related controls
- Guiding principles
- Individual awareness steps
- Etc.

Human Factors

- Guidance on day-to-day use of technology
- Usability controls
- Fault/error-tolerant systems
- Complexity reduction
- Controls addressing specific behaviors
- Etc.

Emergence

- Responsible use
- Controls addressing habitual behavior
- Change management controls
- Feedback on user understanding
- Continuous improvement controls
- Etc.





Figure 6—COBIT 5 Enabler: Systemic Model With Interacting Enablers

Processes

Describe an organised set of practices and activities to achieve certain objectives and produce a set of outputs in support of achieving overall IT-related goals

Organisational Structures

Are the key decision-making entities in an enterprise

Culture, Ethics and Behaviour

Relate to individuals and the enterprise and are often underestimated as a success factor in governance and management activities



Principles, Policies and Frameworks

Are the vehicles to translate the desired behaviour into practical guidance for day-to-day management



Deals with all information produced and used by the enterprise. Information is required for keeping the organisation running and well governed.

At the operational level, information is also often the key product of the enterprise itself.

Services, Infrastructure and Applications

Include the infrastructure, technology and applications that provide the enterprise with IT processing and services

People, Skills and Competencies

Are linked to people required for successful completion of all activities for making correct decisions and taking corrective actions

RESOURCES





INTERNAL CONTROL (COSO 2013)

Internal control is defined as follows:

Internal control is a process, effected by an entity's board of directors, management, and other personnel, designed to provide reasonable assurance regarding the achievement of objectives relating to operations, reporting, and compliance.





HUBUNGAN ANTAR KERANGKA

Tata Kelola TI

PP60/2008

Sistem Pengendalian Intern

ernal Control mework COSO

Panduan Umum Tata Kelola TIK Nas

+

Kuesioner Evaluasi Pengendalian Intern TIK

COBIT

SNI ISO 38500

SNI ISO 20000

SNI ISO 27001

Manajemen





PERATURAN PEMERINTAH RI NO 60/2008 SPIP

BABII

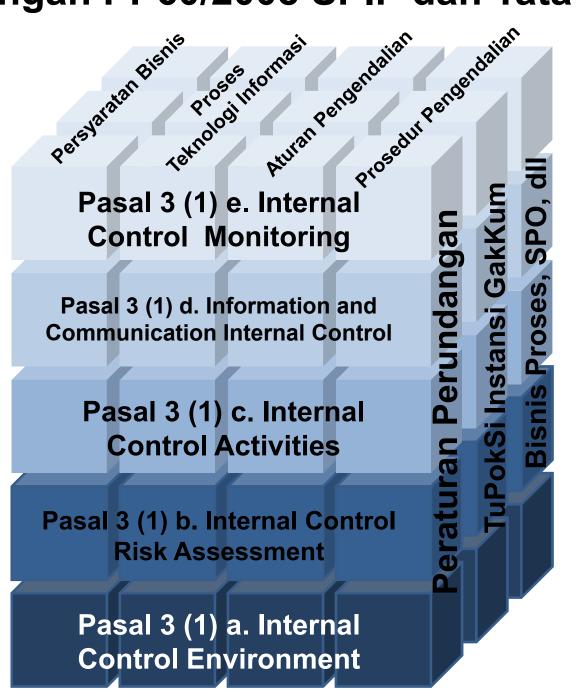
UNSUR SISTEM PENGENDALIAN INTERN PEMERINTAH

Bagian Kesatu Umum

Pasal 3

- SPIP terdiri atas unsur:
 - a. lingkungan pengendalian;
 - b. penilaian risiko;
 - kegiatan pengendalian;
 - d. informaci dan komunikaci; dan
 - e. pemantauan pengendalian intern.
- (2) Penerapan unsur SPIP sebagaimana dimaksud pada ayat (1) dilaksanakan menyatu dan menjadi bagian integral dari kegiatan Instansi Pemerintah.

Hubungan PP60/2008 SPIP dan Tata Kelola TI



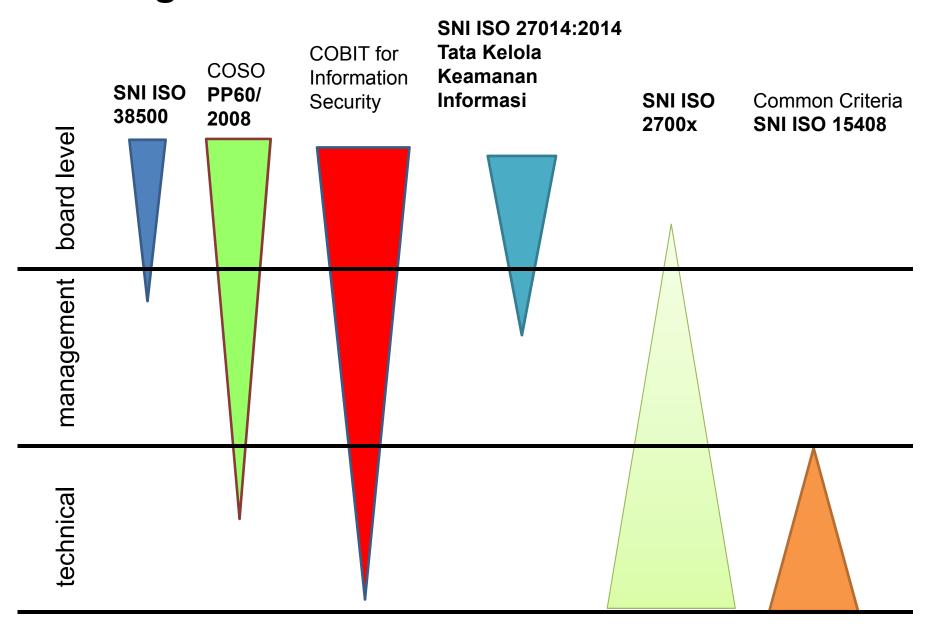
PP60/2008 Sistem Pengendalian Intern Pemerintah

Tata Kelola Teknologi Informasi, PUTK-TIK Nas + KEPI-TIK v1.2.1

Best Practice (Operasional)

SNI ISO 20000-1 Manajemen Layanan Teknologi Informasi SNI ISO/IEC 27001 Sistem Manajemen Keamanan Informasi

Kerangka dan Standar Keamanan Informasi



SERI SNI 15408 – KRITERIA EVALUASI KEAMANAN TI

ISO/IEC 15408-1:2009 Evaluation criteria for IT security - Part 1: Introduction and general model

SNI ISO/IEC 15408-1:2013 Teknologi informasi - Teknik keamanan - Kriteria evaluasi keamanan teknologi informasi - Bagian 1: Pengantar dan model umum

ISO/IEC 15408-2:2008 Evaluation criteria for IT security - Part 2: Security functional components

SNI ISO/IEC 15408-2:2013 Teknologi informasi - Teknik keamanan - Kriteria evaluasi keamanan teknologi informasi - Bagian 2: Komponen fungsional keamanan

ISO/IEC 15408-3:2008 Evaluation criteria for IT security - Part 3: Security assurance components

SNI ISO/IEC 15408-3:2013

Teknologi informasi - Teknik keamanan - Kriteria evaluasi keamanan teknologi informasi - Bagian 3: Komponen jaminan keamanan

REFERENCE

ISO, ISO/IEC 22301:2012 Societal security—Business continuity management systems—Requirements

ISO, ISO/IEC 22313:2012 Societal security—Business continuity management systems—Guidance

ISO, ISO/IEC 24762:2008 Information technology—Security techniques—Guidelines for information and communications technology disaster recovery services

ISO, ISO/IEC 27001:2013 Information technology—Security techniques—Information security management systems—Requirements

ISO, ISO/IEC 27005:2011 Information technology—Security techniques—Information security risk management.

ISO, ISO/IEC 27031:2011 Information technology—Security techniques—Guidelines for information and communication technology readiness for business continuity.

ISO, ISO/IEC 27032:2012 Information technology—Security techniques—Guidelines for cybersecurity.

ISO, ISO/IEC 31000:2009 Risk management—Principles and guidelines.

ISACA, Advanced Persistent Threat Awareness Study Results, USA, 2014,

www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Advanced-Persistent-ThreatsAwareness-Study-Results.aspx

ISACA, COBIT® 5, USA, 2012, www.isaca.org/COBIT/Pages/COBIT-5-Framework-product-page.aspx

ISACA, COBIT® 5 for Assurance, USA, 2013, www.isaca.org/COBIT/Pages/Assurance-product-page.aspx

ISACA, COBIT® 5 for Information Security, USA, 2013, www.isaca.org/COBIT/Pages/Information-Security-Product-Page.aspx

ISACA, COBIT® 5 for Risk, USA, 2013, www.isaca.org/COBIT/Pages/Risk-product-page.aspx

ISACA, European Cybersecurity Implementation: Assurance, USA, 2014

ISACA, European Cybersecurity Implementation: Audit Programme, USA, 2014

ISACA, European Cybersecurity Implementation: Resilience, USA, 2014

ISACA, European Cybersecurity Implementation: Risk Guidance, USA, 2014

ISACA, Responding to Targeted Cyberattacks, USA, 2013, www.isaca.org/Knowledge-

Center/Research/ResearchDeliverables/Pages/Responding-to-Targeted-Cyberattacks.aspx

ISACA, Transforming Cybersecurity, USA, 2013







Discussion

www.isaca.org/cyber

Email: csx@isaca.or.id

