

มาตรฐานเทคโนโลยีสารสนเทศ

รอม หิรัญพฤษ

อ.กพร. รัฐบาลอิเล็กทรอนิกส์

สำนักงานพัฒนาวิทยาศาสตร์และเทคโนโลยีแห่งชาติ

กระทรวงวิทยาศาสตร์และเทคโนโลยี

หัวข้อบรรยาย

- **ทำไมต้องมีมาตรฐาน ICT**
- **มาตรฐานเกี่ยวกับบุคคล**
- **มาตรฐานกระบวนการ/องค์กร**
- **มาตรฐานการควบคุม**
- **มาตรฐานเปิด (open standards)**

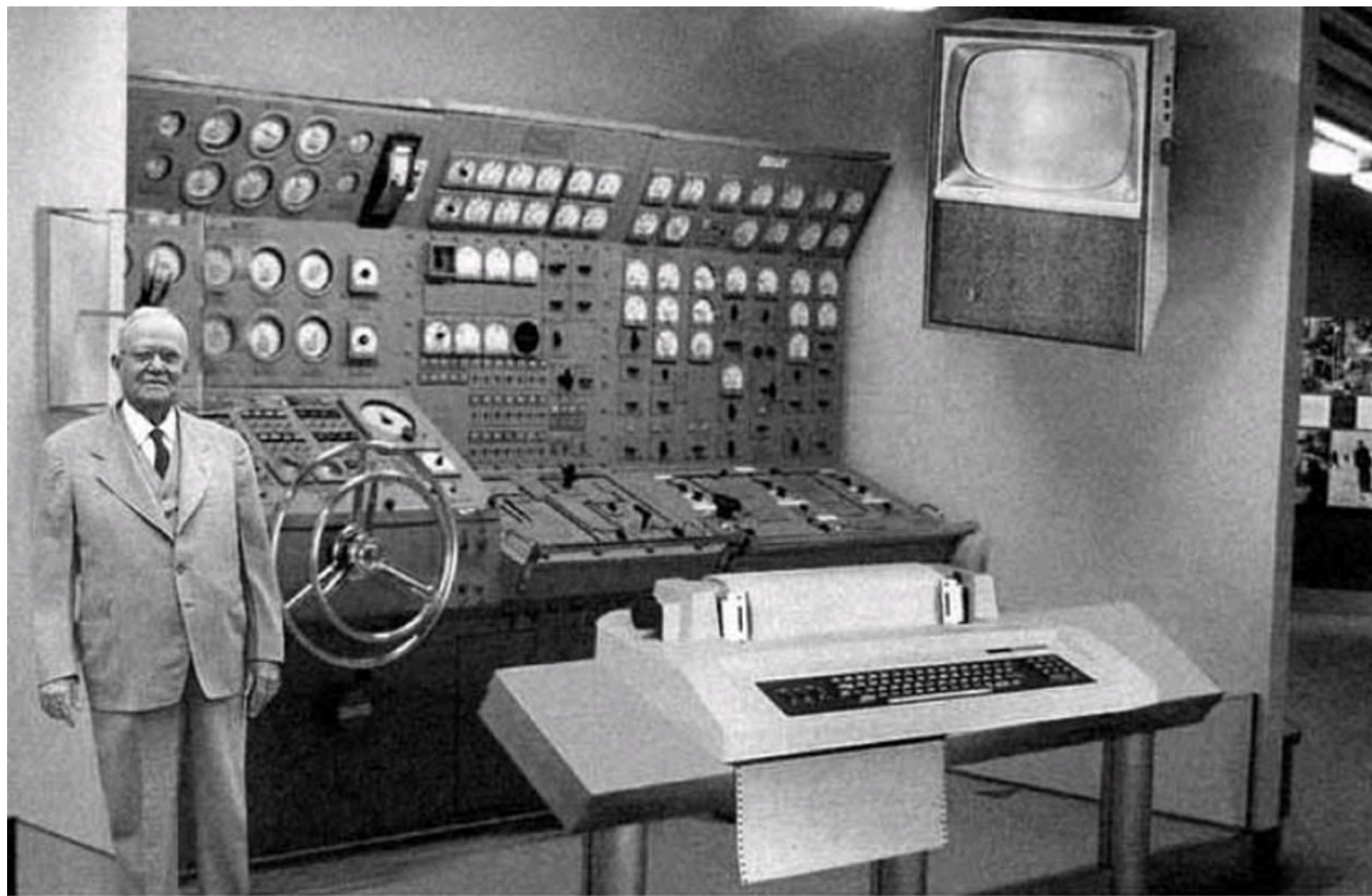
IT Contribution to GDP Growth Per Hour worked

Figure 1

IT Contributions

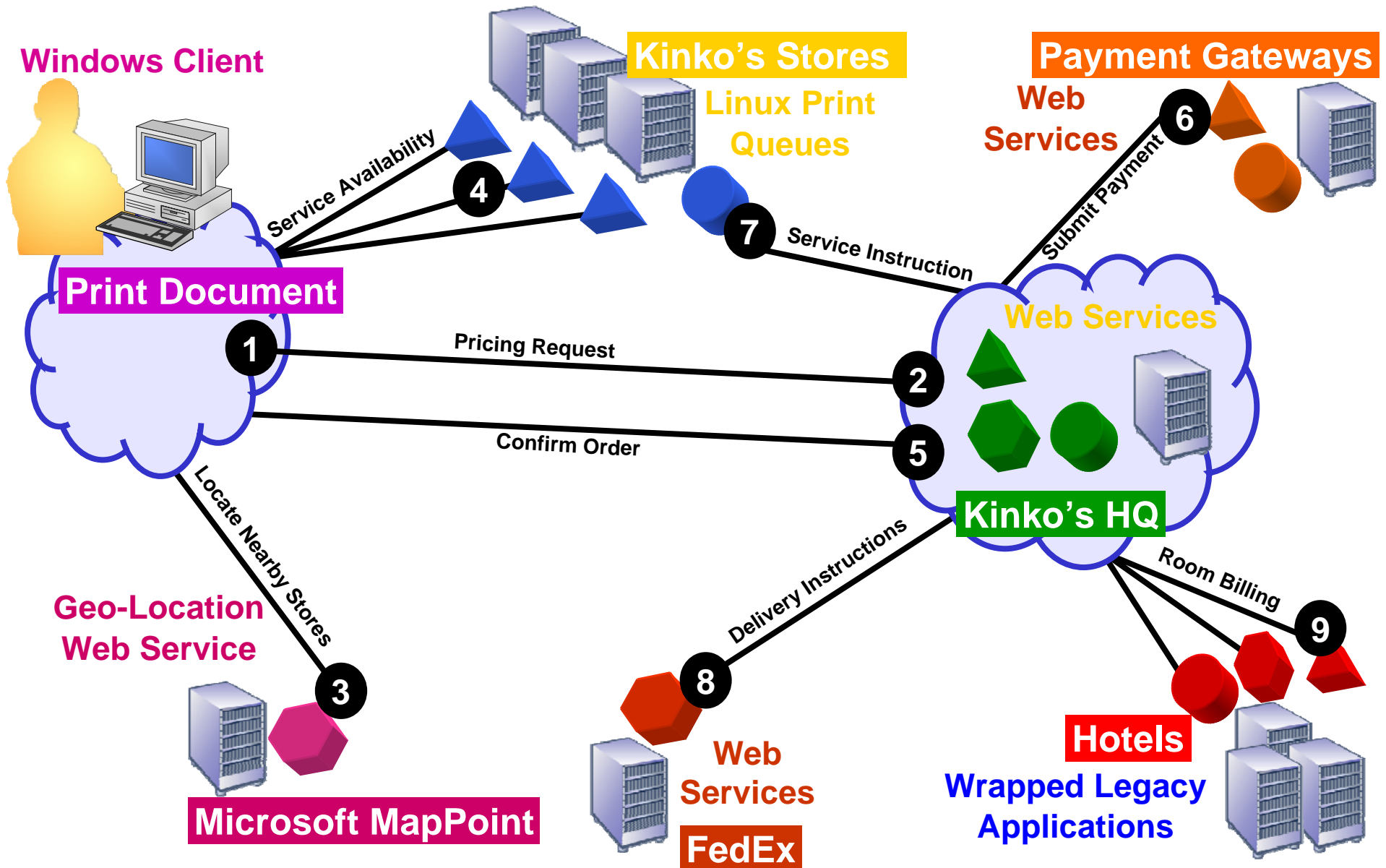


SOURCE: NASSCOM



Scientists from the RAND Corporation have created this model to illustrate how a "home computer" could look like in the year 2004. However the needed technology will not be economically feasible for the average home. Also the scientists readily admit that the computer will require not yet invented technology to actually work, but 50 years from now scientific progress is expected to solve these problems. With teletype interface and the Fortran language, the computer will be easy to use.

มาตรฐานทำงานร่วมกัน: Kinkos (Source: StatETech 2007)



ทำไมต้องพัฒนาและใช้มาตรฐาน

- ทำให้ทำงานร่วมกันได้ (interoperate) มีภาษาและความเข้าใจตรงกัน
- ทำให้มีเกณฑ์กลางในการทำงาน การบริการ แลกเปลี่ยนข้อมูล และรักษาความมั่นคง
- สำหรับผู้ใช้หรือผู้ซื้อเป็นการลดความเสี่ยง
- ทำให้ทำงานข้ามระบบได้ (interoperability)
- ลดอุปสรรคทางการค้า

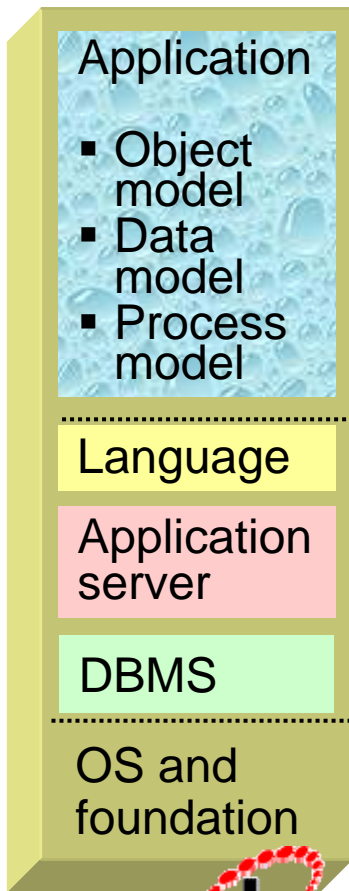


วิธีทำให้เกิด **Interoperability**

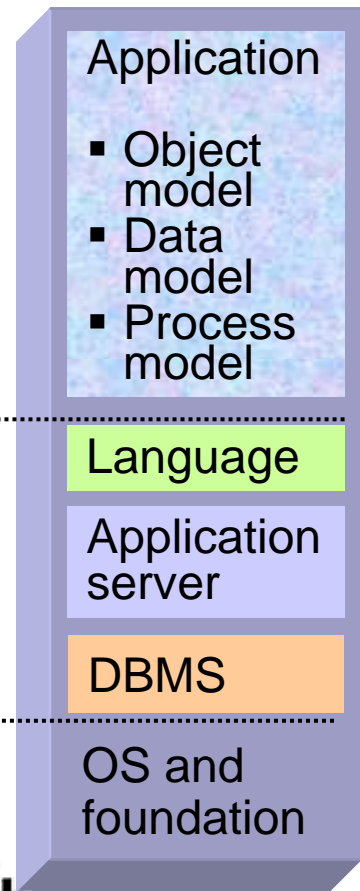
- Product design (PDF vs. I-Pod)
- By licensing and cross-licensing IP (Patent Pooling, MSFT-Novell deal)
- By open innovation and collaborative R&D
- By implementing standards
- By government mandates

Key Trend: Standards are Evolving Up The Stack

Application 1



Application 2



Application Level:
Data, business process, orchestration, semantics

Middleware:
Web services, JMS, J2EE, .NET, CORBA, IIOP, SQL, JDBC, ODBC

Network: TCP/IP, other

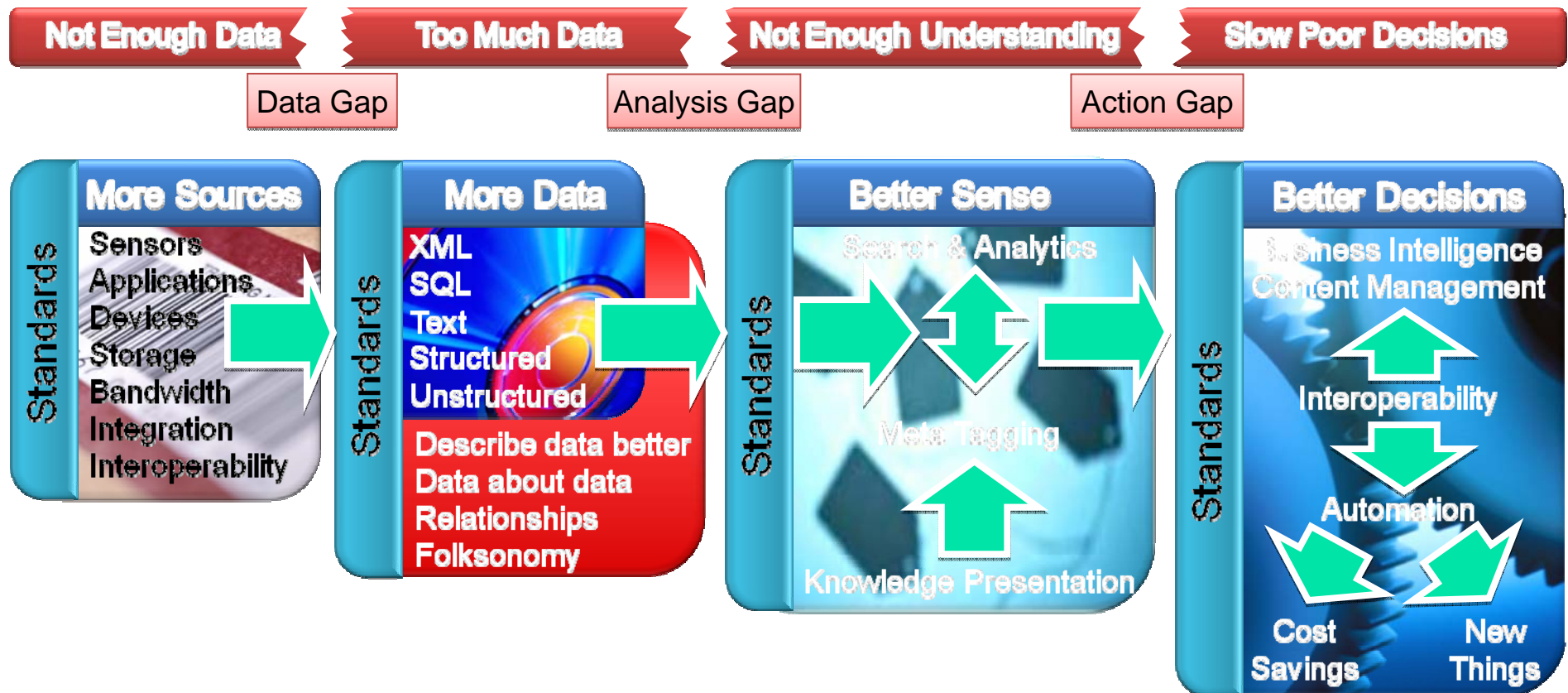
Application Integration
Interoperability

มาตรฐานต่างจากบูรณาการ

- **Integration** is like trying to force a square box to fit into a round hole
 - Working together with others was an afterthought, not part of design.
- **Interoperability** is about designing to work with other unknown elements from the outset

Standards at Work: Addressing a Major Issue – Volume of Data

By 2015 the average company will have 30 times more data to deal with than in 2007.



มาตรฐานสำคัญอย่างไร (ที่มา: ครรชิต มัลลียงค์)

- เป็นเกณฑ์สำหรับ
 - วิธีปฏิบัติที่ดีที่สุด
 - งานที่มีประสิทธิภาพและได้ผล
 - ความสามารถบุคคล/องค์กร
 - การทำงานร่วมกัน
 - การกำหนดระดับความยอมรับ

มาตรฐานด้าน ICT

- เกิดขึ้นอย่างรวดเร็ว
- เป็นเกณฑ์สำหรับ
 - อุปกรณ์และเครื่องมือ
 - การต่อเชื่อมและโปรโตคอล
 - ภาษาและอักษร
 - การจัดการและบริการ
 - ความมั่นคงและความเชื่อถือได้
 - ข้อมูลและบันทึก
 - ฯลฯ

มาตรฐานโลก

Key Standardization Areas

- **Audio/Video compression**
– MPEG, JPEG
- **Computer Media** – DVD, CD, Magnetic Tape
- **Programming Languages**
– COBOL, Fortran, C, C++
- **System Interfaces** -
POSIX
- **Software and Systems Engineering**
- **Character Sets**
- **Databases**
- **Security and Biometrics**
- **Systems and Device Interconnection** – SCSI
- **Credit Cards, “Smart” Cards, Machine-readable Travel Documents**
- **Learning Technologies**

ประเทศไทยกำลังทำอะไร

- **สมอ.ได้สร้างมาตรฐานไทยหลายด้าน**
 - **Keyboard layout**
 - **Thai character codes (8 and 16 bits)**
 - **EDI**
 - **GIS**
 - **ฯลฯ**

สมอ.และมาตรฐานโลก

- **สมอ.ได้ใช้การยอมรับมาตรฐานโลกหลายประเภทมาใช้เป็นของไทย เช่น**
 - **Graphic**
 - **Protocol**
 - **Hardware standards**
 - **Telecommunications**
 - **ฯลฯ**

Industry Specifications

- **Morse code 1844**
- **ITU : standard telegraph protocol**
- **IEEE, ETSI, ECMA, ANSI**
- **EIDX (Electronics Industry Data Exchange,)**
- **SWIFT Banking secure messaging standard**
- **EDI (EDIFACT/X120)**
- **Over time, *specifications* may become *standards***
- **Industry creates standards**
- ***BUT* no guarantee of success;-**
 - **VHS – Betamax (done deal!)**
 - **Metric vs. Imperial (ongoing!!)**
 - **Blue Ray vs. HD-DVD (just started!)**

Some leads to STANDARDS

กระบวนการในการเกิดของมาตรฐาน

- The Idea > - From Industry or Academia***
- Prototype > - The creative moment (IPR)***
- Beta > - The test of innovation***
- Roll out > - does the market want it?***
- Early adoption > - will the market use it?***
- Critical mass > - The undefined measure of 'success'***
- National/International industry consortium > - Critical Peer Review***
- ISO/ITU open standards Org > - International Technical Review***
- GLOBAL STANDARD > - Availability to all on RAND **or** RF terms***

Leading to interoperability

ทางเลือกสำหรับมาตรฐาน

- **Open Standards**
 - Voluntary private sector initiatives, e.g. WS-I, W3C, OASIS
 - Government specification, e.g. European Interoperability Framework
 - Private - Public multi stakeholder partnerships
- **Organic (market driven) Standards**
 - บาง specifications ได้กลายเป็นมาตรฐานกลางสำหรับ interoperability – ทั้งที่เป็นของบริษัทเดียว เช่น PDF
- ตลาดจะตอบสนองการยอมรับของผู้ใช้ เช่น Microsoft ก็ได้รับรอง Linux ผ่านบริษัทพันธมิตร เช่น – Novell สนับสนุน Open XML ในระบบ Linux ตั้งแต่ Jan 2007: IBM ก็มีการรองรับ Linux มาแล้วหลายปี

วิธีเลือกมาตรฐานในการจัดซื้อ

- cost-benefit analysis (CBA)
- Total Cost of Ownership (TCO)

TCO คำนวณจากค่าจัดซื้อของสินค้าและบริการ + 'hidden costs' ในการใช้ระบบ ICT ซึ่งรวมถึงค่าใช้จ่ายที่เกี่ยวกับ planning, design, installation, configuration, maintenance and support.

แนวคิดสำหรับการจัดซื้อ

- 1. Technology Neutrality**
 - maintains choice – lowers prices
- 2. Encompass Industry Standards**
 - Interoperability and consumer acceptance
- 3. Foster Strong Intellectual Property Protection**
 - sustainable development and lasting value

ประเทศไทย

- ประเทศไทยกำลังยอมรับมาตรฐานโลกมาใช้มากขึ้นเรื่อยๆ
- หน่วยงานที่กำลังทำงานด้านนี้
 - TISI
 - Software Industry Promotion Agency
 - Software Park Thailand
 - NECTEC
 - ATCI, ATSI

ตัวอย่างมาตรฐานบุคคลเกี่ยวข้องกับ IT

- **Certified Information Systems Auditor (CISA)**
- **Certified Information Systems and Security Professional (CISSP)**
- **Certified Software Project Manager (CSPM)**
- **Certified Software Quality Analyst (CSQA)**
- **Certified Software Tester (CSTE)**
- **มาตรฐานเฉพาะทางของบริษัท ICT**
- **มาตรฐานเฉพาะทางของภาครัฐ**

Department of Defense (DOD) Directive 8570.1 ; Standard for Security Certified Professional

- กระทรวงกลาโหมสหรัฐ (DOD) ได้ออกมาตรฐานขั้นต่ำเกี่ยวกับประกาศนียบัตรผู้เชี่ยวชาญด้านความปลอดภัยข้อมูลสำหรับข้าราชการประจำ และ Contractor ต่างๆ ที่การปฏิบัติงานมีความจำเป็นต้องเข้าถึงข้อมูลของ DOD ซึ่งแบ่งลักษณะของประกาศนียบัตรออกเป็น 2 ระดับ คือ ระดับเทคนิค และระดับบริหาร (Technical and Management) ซึ่งในระดับเทคนิคยังแบ่งเป็น Technical I, II, III และระดับบริหารแบ่งเป็น Management I, II, III
- สำหรับ Security Certification ที่ได้รับการยอมรับจาก DOD เช่น CompTIA Security + และ (ISC)2 SSCP อยู่ในระดับ Technical II ส่วน CISSP, CISA และ GIAC อยู่ในระดับ Technical III สำหรับระดับ Management I ได้แก่ Security + และระดับ Management II และ III ได้แก่ CISSP, CISM และ GIAC



IA Workforce Certifications

Proposed Certifications

Technical I	Technical II	Technical III
A+ Network+ TICSA SSCP	GSEC Security+ SCNP SSCP	CISSP SCNA CISA GSE
Management I	Management II	Management III
GSLC Security+ GISO TISCP	CISSP GSLC CISM	CISSP GSLC CISM

ตัวอย่างมาตรฐานบุคลากรของบริษัทเอกชน

Microsoft

- **MCSE** Microsoft Certified Systems Engineers
- **MCDST** Microsoft Certified Desktop Support Technicians
- **MCSA** Microsoft Certified Systems Administrators
- **MCDBA** Microsoft Certified Database Administrators
- **MCT** Microsoft Certified Trainers
- **MCAD** Microsoft Certified Application Developers
- **MCAD** Microsoft Certified Application Developers
- **MCP** Microsoft Certified Professional Developer
- **Microsoft Office Specialist**

Sun Microsystems

Java SE

- Sun Certified Associate (SCIA)
- Sun Certified Programmer (SCIP)
- Sun Certified Developer (SCID)

Java EE

- Sun Certified Web Component Developer (SCWCD)
- Sun Certified Business Component Developer (SCBCD)
- Sun Certified Developer for Java Web Services (SCDJWS)

Java ME

- Sun Certified Enterprise Architect (SCEA)

Cisco

Associate:

- CCNA Cisco Certified Network Associate
- CCDA Cisco Certified Design Associate

Professional:

- CCNP Cisco Certification network professional

Expert:

- CCIE Cisco Certified Internetwork Expert

Oracle

- OCM Oracle Certified Master
- OCP Oracle Certified Professional
- OCA Oracle Certified Associate

มาตรฐานองค์กร/กระบวนการ

- **แนวโน้มสำคัญคือกลุ่มต่อไปนี้**
 - **CMMI for software development**
 - **SPICE for software development**
 - **ITIL and ISO 20000 for IT Service Management**
 - **ISO 17799 and 27000 for Security**

CMMI คืออะไร

- CMMI (Capability Maturity Model Integration) คือตัวแบบการพัฒนากระบวนการ (ที่วัดทั้งด้านขีดความสามารถและวุฒิภาวะ) ถูกสร้างขึ้นที่ Software Engineering Institute, Carnegie Mellon University
- CMMI เป็นการต่อยอดจาก SW-CMM ที่ใช้แพร่หลายทั่วโลกกับงานพัฒนาซอฟต์แวร์มาจนหมดวาระไปใน 2005
- งานสาขาอื่นๆได้ถูกรวมเข้าใน CMMI ด้วย
- Software Park Thailand ได้เริ่มนำ SW-CMM มาสู่ธุรกิจซอฟต์แวร์ไทยตั้งแต่ 1999 และมีบริษัทได้ SW-CMM ระดับต่างๆราว 20 บริษัทถึงปัจจุบัน ขณะนี้กำลังส่งเสริมการเข้าสู่ CMMI

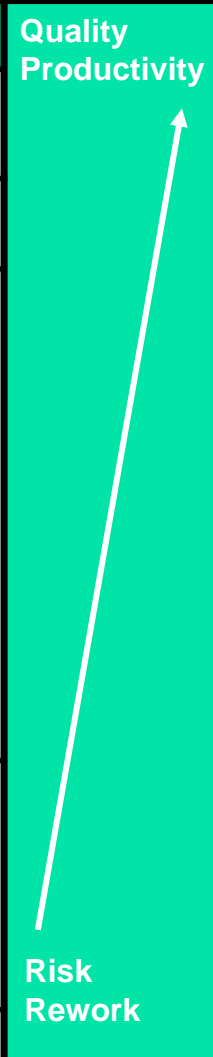
CMMI สามารถใช้กับ

- **Software Engineering**
- **Hardware Engineering**
- **System Engineering**
- **Integrated Product and Process Development Addition**

Process Area ของ CMMI

Category	Process Areas
Process Management	Organizational Process Focus Organizational Process Definition Organizational Training Organizational Process Performance Organizational Innovation and Deployment
Project Management	Project Planning Project Monitoring and Control Supplier Agreement Management Integrated Project Management for IPPD Risk Management Quantitative Project Management
Engineering	Requirements Management Requirements Development Technical Solution Product Integration Verification Validation
Support	Configuration Management Process and Product Quality Assurance Measurement and Analysis Decision Analysis and Resolution Causal Analysis and Resolution

ระดับวุฒิภาวะของ CMMI

Level	Focus	Process Areas	Quality Productivity
5 Optimizing	<i>Continuous Process Improvement</i>	Organizational Innovation and Deployment Causal Analysis and Resolution	
4 Quantitatively Managed	<i>Quantitative Management</i>	Organizational Process Performance Quantitative Project Management	
3 Defined	<i>Process Standardization</i>	Requirements Development Technical Solution Product Integration Verification Validation Organizational Process Focus Organizational Process Definition Organizational Training Integrated Project Management for IPPD Risk Management Decision Analysis and Resolution	
2 Managed	<i>Basic Project Management</i>	Requirements Management Project Planning Project Monitoring and Control Supplier Agreement Management Measurement and Analysis Process and Product Quality Assurance Configuration Management	
1 Initial			

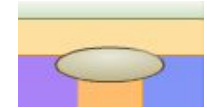
ISO/IEC 20000

- **ISO/IEC 20000 (เดิมคือ BS 15000) ใช้อัปกับ IT Service Management เป็นตัวระบุกระบวนการด้านการจัดการและความต้องการของงาน หรือ ITIL (IT Infrastructure Library)**



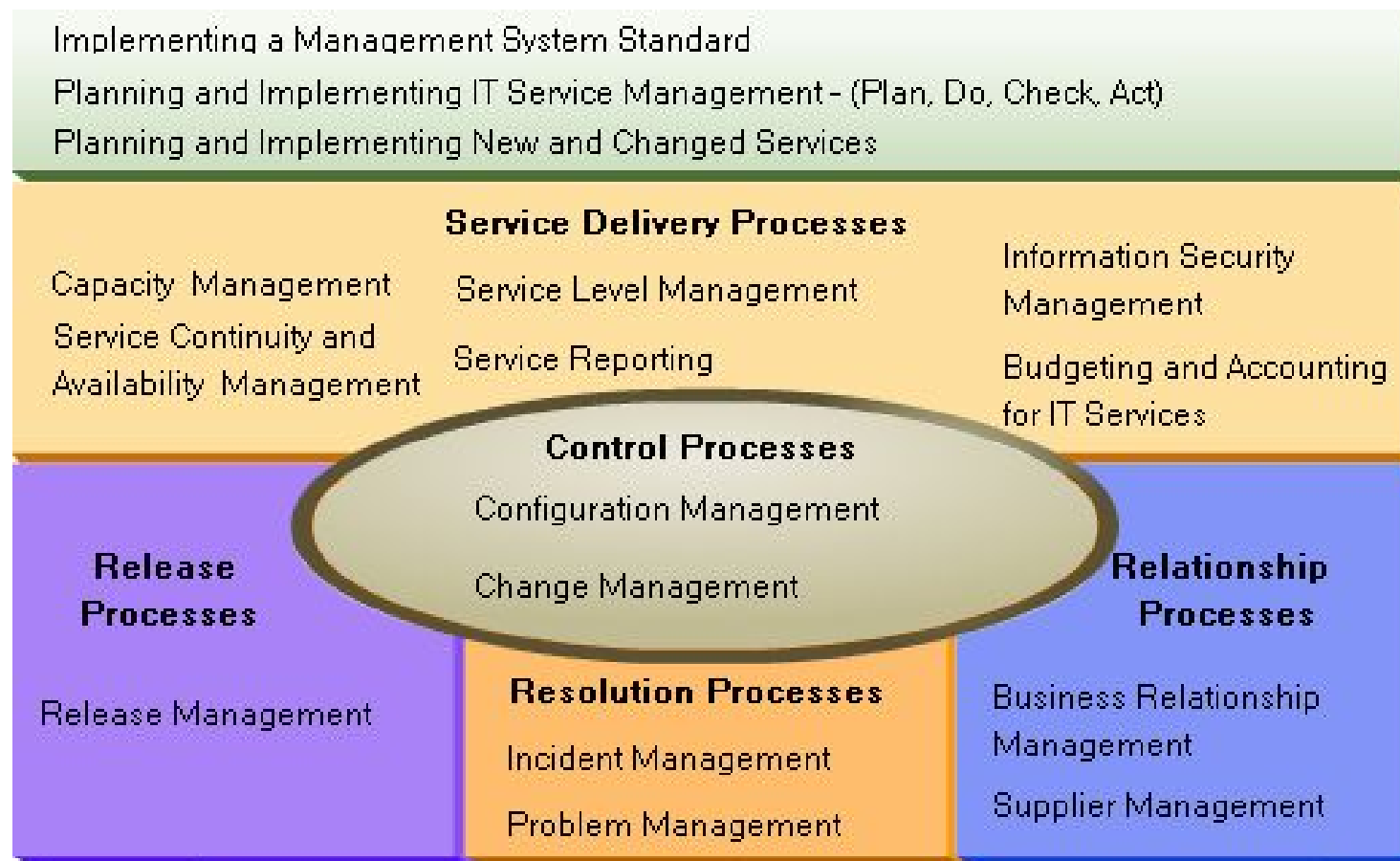
ประเทศไทยกับ ISO/IEC 20000

**เริ่มมีบริษัทไทยทำมาตรฐาน ISO/IEC 20000 เพื่อทำ
ให้บริการด้าน ICT มีคุณภาพและประสิทธิภาพมากขึ้น
มักเป็นองค์กรขนาดใหญ่**



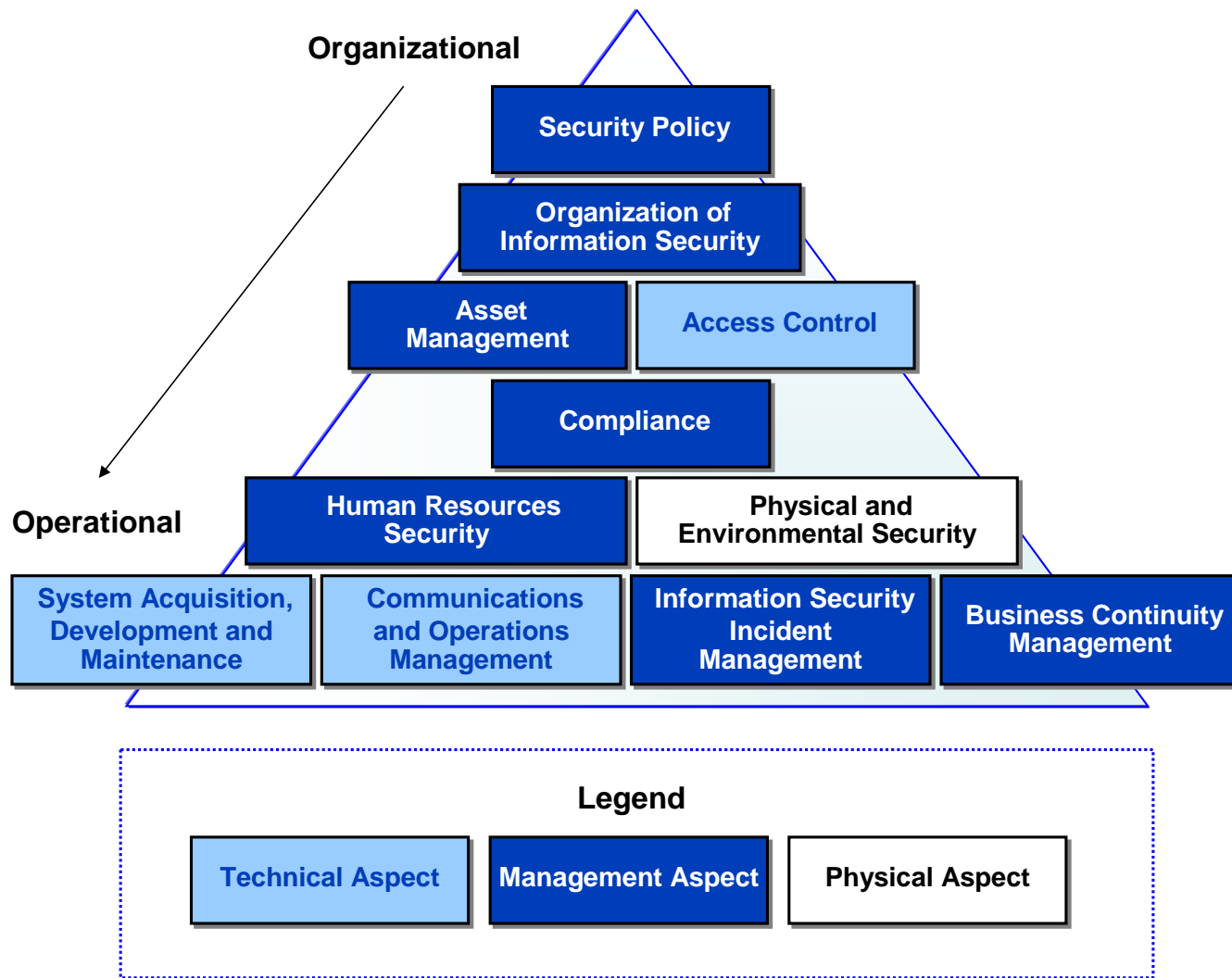
กระบวนการ ISO/IEC 20000

In ISO/IEC 20000, IT service management processes are broadly split into closely linked groups of processes.

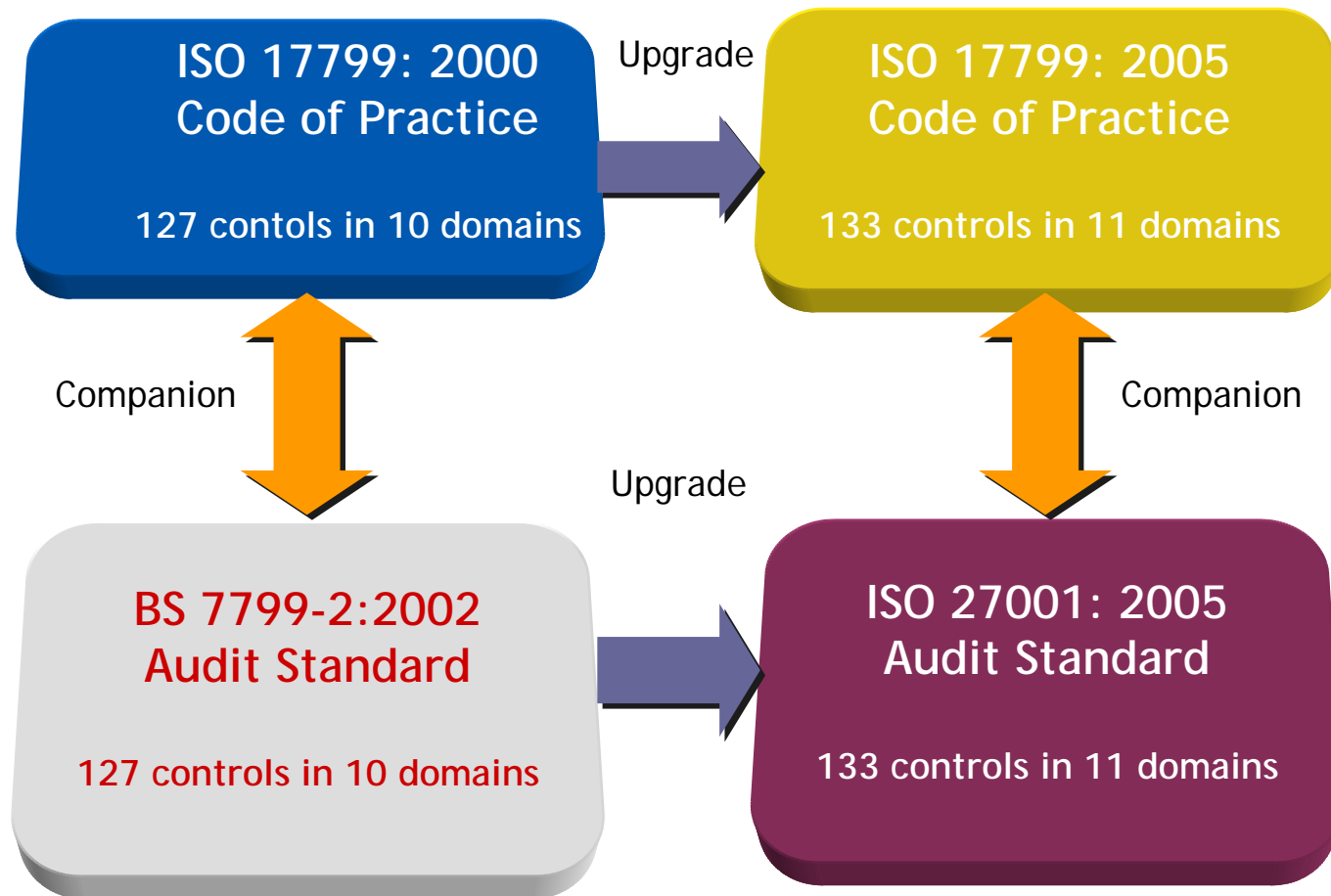


ISO 17799 และ ISO 27000

- **ความมั่นคงด้าน ICT เป็นเรื่องสำคัญสำหรับองค์กรธุรกิจ โดยเฉพาะกับงานการเงินทุกประเภท**
- **NECTEC เป็นเลขานุการ คณะกรรมการธุรกรรมอิเล็กทรอนิกส์**
- **ขณะนี้ไม่มีก็องค์กรที่ผ่านการประเมินเป็นทางการ**



BS 7799 / ISO 17799 / ISO 27001



มาตรฐานกลางด้านความปลอดภัยข้อมูลของ MITRE

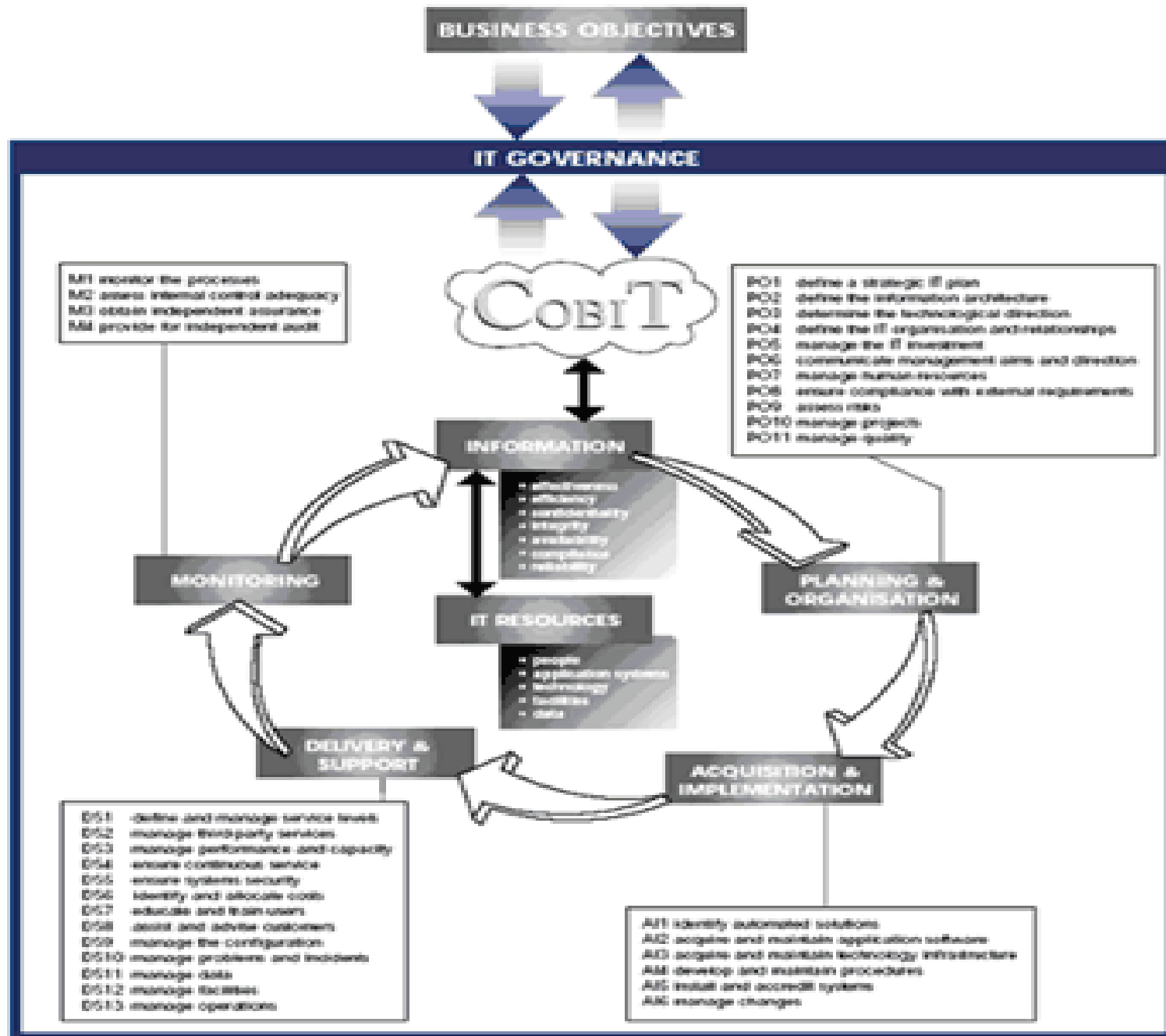
- **OVAl (Open Vulnerability and Assessment Language)**
- **CME (Common Malware Enumeration)**
- **CWE (Common Weakness Enumeration)**
- **CVE (Common Vulnerabilities and Exposures)**

มาตรฐานการควบคุม

COSO and COBIT are - among other things - control frameworks. COSO focuses on controls for financial processes, and COBIT focuses on IT.

- **COSO**
The official name for COSO is the Committee of Sponsoring Organizations of the Treadway Commission.
- **COSO framework materials** are available from the American Institute of Certified Public Accountants.
- **COSO Enterprise Risk Management Framework.**
- **COBIT**
COBIT (Control Objectives for Information and Related Technologies) is an open standard published by the **IT Governance Institute** and the Information Systems Audit and Control Association (ISACA). It's an IT control framework built in part upon the COSO framework.

The latest version of COBIT is COBIT 4.0.



The New Innovation Process

From: Henry Chesbrough, "Open Innovation, the New Imperative for Creating Profit from Technology",
Harvard Business School Press, 2006

Closed Innovation

The smart people in our field work for us

To profit from R&D, we must discover it, develop it, and ship it ourselves

If we discover it ourselves, we will get it to market first

The company that gets an innovation to market first will win

If we create the most and best ideas in the industry, we will win

We should control our IP, so that our competitors don't profit from our ideas

Open Innovation

Not all the smart people work for us. We need to work with smart people inside and outside the company

External R&D can create significant value; internal R&D is needed to claim some portion of that value

We don't have to originate the research to profit from it

Building a better business model is better than getting to market first

If we make the best use of internal and external ideas, we will win

We should profit from others' use of our IP, and we should buy others' IP whenever it advances our own business model

Open Standards

- Open standards are a set of technical specifications, developed or approved through a consensus process, that are widely reviewed and agreed upon, and are published in sufficient detail to permit a variety of implementations, and publicly available.
- **The open standards process is a collaborative effort, which mirrors the open innovation process. By helping to achieve industry consensus around standards that reflect cutting edge technologies, this process produces standards always superior to government mandated standards.**

แนวคิดเกี่ยวกับมาตรฐานเปิด

- Always be royalty free, as opposed to the use of F/RAND criteria;
 - Be controlled by a non-profit “neutral” organization; and
 - Impose no constraints on the re-use of the standard.
-
- **However, it is important to remember that the open standards process can only contribute to interoperability if the resulting standards are adopted.**
 - **Open standards development, without significant global adoption of the resulting standards, does nothing in the effort to achieve interoperability.**