Electronic Transactions Commission

แนวทางการให้บริการ Cloud Computing
(Cloud Service Provider Recommendation)
ภายใต้ประกาศคณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์

Electronic Transactions Commission

ประเด็นที่ผู้ใช้ให้ความสำคัญ 5 อันดันแรกในการใช้ Cloud ?

มาตรฐาน	ความมั่นคงปลอดภัย	ข้อตกลงการให้บริการ (SLA)	ความรับผิดชอบของผู้ให้บริการ
ความน่าเชื่อถือ	การจัดการข้อมูล	ค่าใช้จ่าย	การเลือกใช้งาน
สถานที่เก็บข้อมูล	การคุ้มครองข้อมูล	ประสิทธิภาพการให้บริการ	สำรองข้อมูล

นิยาม Cloud Computing

National Institute of Standard and Technology (NIST)
กำหนดความหมายของบริการ Cloud Computing ครอบคลุมสาระสำคัญใน 3 มิติ

คุณสมบัติของบริการ

On Demand Self Service : สามารถปรับเปลี่ยนการใช้งาน ได้ตามความต้องการในช่วงเวลาใดก็ได้

Broad Network Access: สามารถเข้าใช้ระบบได้จากอุปกรณ์ประเภทใดก็ได้

Resource Pooling: สามารถบริหารจัดการระบบเพื่อให้บริการแก่ผู้ใช้งานจำนวนมากในเวลาเดียวกัน โดยไม่ต้องรู้แหล่งที่จัดเก็บ

Rapid Elasticity: มีความยืดหยุ่นสูงตามความต้องการของผู้ใช้งาน สามารถเพิ่มหรือลดทรัพยากรได้เร็ว ไม่มีข้อจำกัดเรื่องจำนวน ปริมาณ และระยะเวลาในการใช้งาน

Measured Service: การวัดปริมาณและคิดค่าบริการตามการใช้งานที่เกิดขึ้นจริง หรือ Pay per use

ประเภทการให้บริการ

Infrastructure as a Service : IaaS
การให้บริการโครงสร้างพื้นฐานหลักของบริการ Cloud Computing เช่น ระบบประมวลผล ระบบจัดเก็บข้อมูล ระบบเครือข่าย โดยผู้ใช้ไม่ต้องบริหารจัดการโครงสร้างพื้นฐานเอง

Platform as a Service : PaaS
การให้บริการแพลตฟอร์ม และเครื่องมือเพื่อใช้ในการพัฒนาซอฟต์แวร์แอพพลิเคชั่น เช่น โปรแกรมเบื้องต้น ฐานข้อมูล โดยผู้ใช้ไม่ต้องบริหารจัดการระบบเอง แต่ต้องติดตั้ง แก้ไข ปรับแต่งแอพพลิเคชั่นที่สร้างหรือพัฒนาขึ้นเอง

Software as a Service : SaaS
การให้บริการซอฟต์แวร์ที่มีความยืดหยุ่นต่อการใช้เข้างานได้หลากหลาย โดยผู้ใช้ไม่ต้องบริหารจัดการเอง

รูปแบบของบริการ

Private Cloud : บริการสำหรับหน่วยงานหรือองค์กรใดองค์กรหนึ่งเพียงองค์กรเดียว

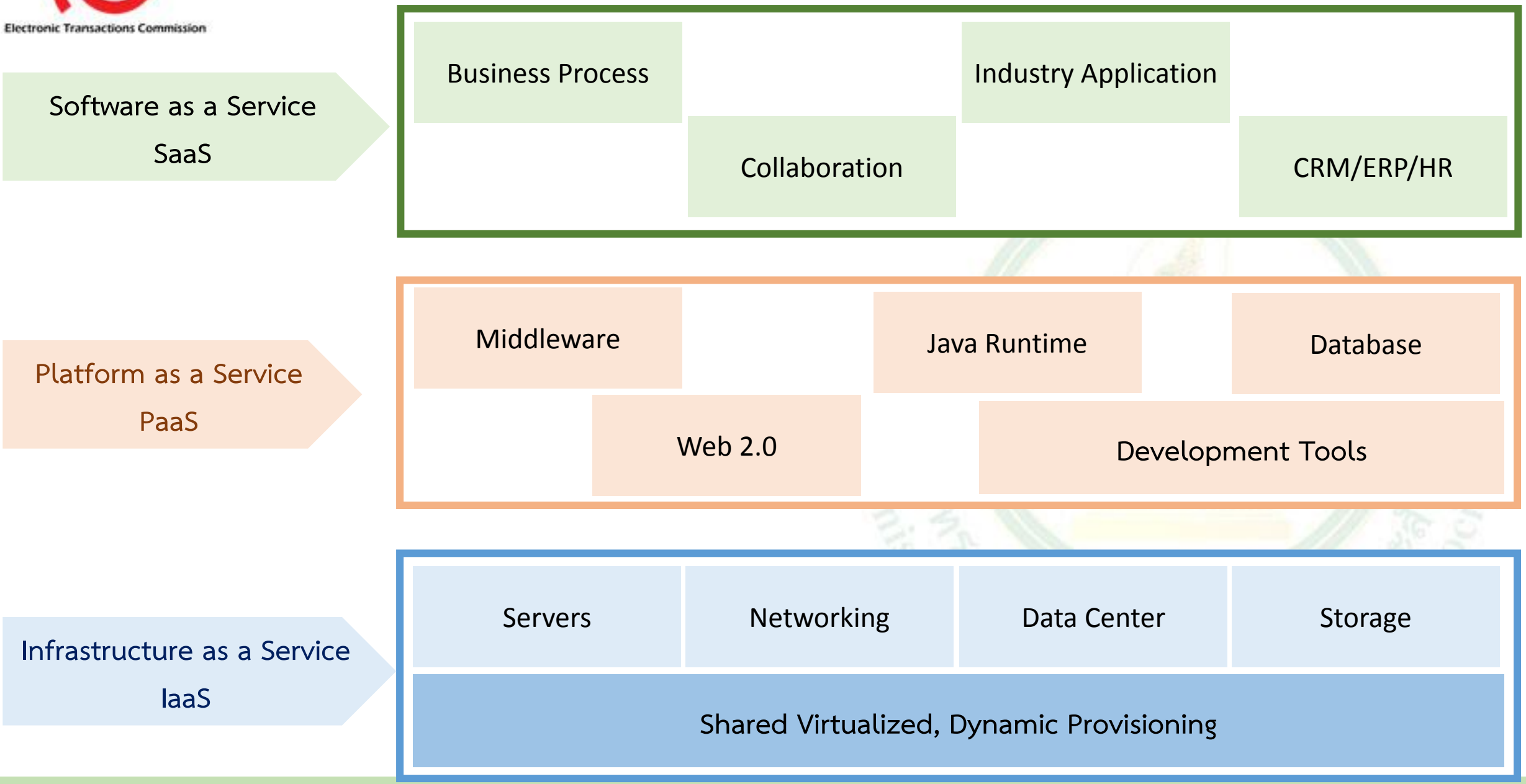
Community Cloud : บริการที่ดำเนินการร่วมกันโดยกลุ่มคนที่มีการรวมตัวกันอยู่ในรูปแบบของการจัดตั้งเป็นสมาคม ชมรม ทั้งเป็นทางการหรือไม่เป็นทางการ โดยมีความต้องการใช้บริการแบบเดียวกัน

Public Cloud : บริการที่เปิดให้สาธารณชนและหน่วยงานต่างๆ ใช้งานทั่วไป โดยการบริหารจัดการและการให้บริการอาจเป็นบริษัท สถาบันการศึกษา เป็นผู้ให้บริการ

Hybrid Cloud : ผสมผสานรูปแบบการบริการตั้งแต่สองแบบขึ้นไป สำหรับงานเฉพาะกิจ ซึ่งผู้ใช้งานจะต้องมีมาตรฐานคุณสมบัติทางเทคนิคและเทคโนโลยีที่สามารถใช้งานข้อมูลและถ่ายโอนแอพพลิเคชั่น สำหรับการใช้งานข้ามไปมาระหว่างรูปแบบแต่ละแบบที่เลือกใช้

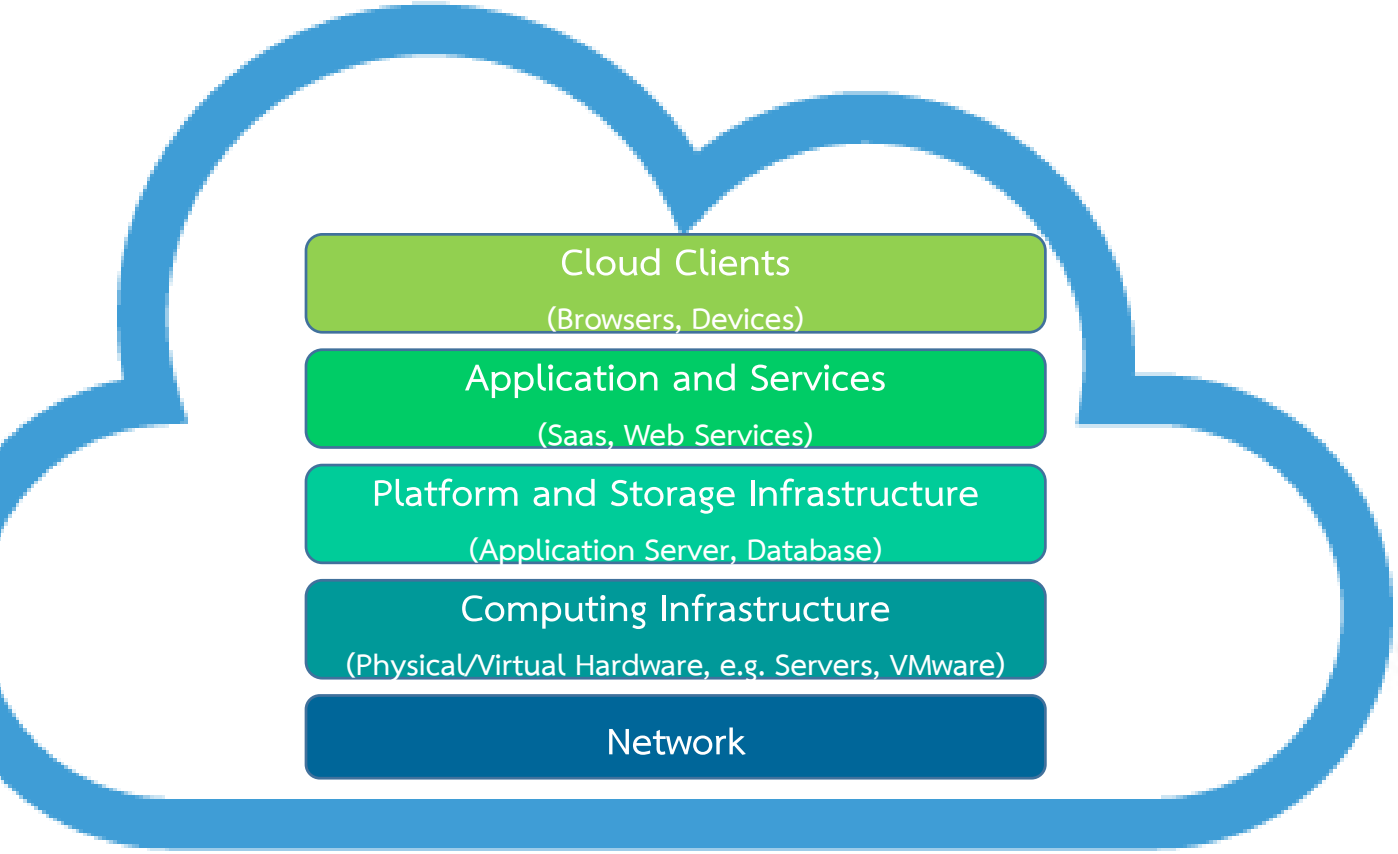
ประเภทการให้บริการของ Cloud Computing

Electronic Transactions Commission



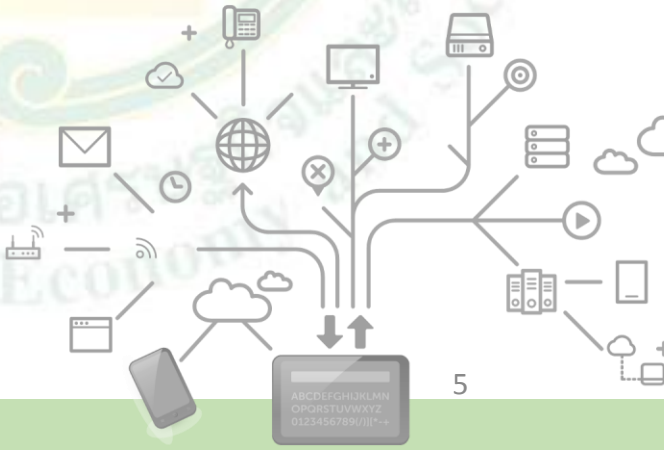
Electronic Transactions Commission

ประเด็นที่เกี่ยวข้องกับการใช้บริการ Cloud Computing



Cloud Computing Stack

- Cross Border Information
- Data Localization
- Privacy
- Security



หลักเกณฑ์การให้บริการ Cloud Computing

Asia Cloud Computing Association
[Cloud Assessment Tool 2012]

Eurocloud Star Audit (ECSA)
[trusted cloud service 4stars]]

ICO. Information Commission Office UK
[Guidance on the use of Cloud Computing 2012]

Performance
Security
Data Protection
Data Management

Hongkong
[Practise Guide for Procuring Cloud Service 2013]

Performance
Security
Data Protection
Data Management

Performance
Security
Data Protection
Data Management

U.S. National Institute of Standards and Technology : NIST
[Guideline on Security and Privacy in Public Cloud 2011]

Performance
Security
Data Protection
Data Management

South Korea
[Act on the Development of Cloud Computing and Protection of Users 2015]

Performance
Security
Data Protection

European commission
[Cloud Service Level Agreement Standardisation Guideline 2014]

Performance
Security
Data Protection
Data Management

New Zealand
[Cloud Computing: Information Security and Privacy Consideration 2014]

Performance
Security
Data Protection
Data Management

India
[Interoperability and Portability for Cloud Computing Guide 2014]

Performance
Security
Data Protection

Australia
[Privacy & Cloud Computing Guideline 2013]

Security
Data Protection
Data Management

Cloud Security Alliance (CSA)

Security

ISO

Security
Data Protection

การดำเนินการด้าน Cloud Computing ของประเทศไทย

Electronic Transactions Commission

ร่างแนวทางการให้บริการ Cloud Computing

ตัวอย่างผู้ให้บริการในประเทศไทย

บริษัท คลาวด์ คอมพิวติ้ง โซลูชั่น จำกัด
บริษัท กสท โทรคมนาคม จำกัด (มหาชน)
บริษัท ทีโอที จำกัด (มหาชน)
บริษัท ไชโย โฮสติ้ง จำกัด
บริษัท ทรู ไอดีซี จำกัด
บริษัท อินเทอร์เน็ตประเทศไทย จำกัด (มหาชน)
บริษัท ดาต้าโปร บิวสิเนส จำกัด
สำนักงานพัฒนารัฐบาลดิจิทัล(องค์การมหาชน)
บริษัท คลาวด์บิสซิเนส จำกัด (VPS)
บริษัท ไทยดาต้าโฮสติ้ง จำกัด
ฯลฯ

ร่างมาตรฐานปฏิบัติการแบบ Cloud

ธนาคารแห่งประเทศไทย

ออกนโยบายการใช้บริการ IT Outsourcing ในการประกอบธุรกิจของสถาบันการเงิน นิยาม กำหนดหลักเกณฑ์การใช้บริการ Cloud Computing

กสท

กำหนดนโยบายการใช้งาน Cloud Computing สำหรับผู้ประกอบการ (วิธีการคัดเลือก ประเมิน การทบทวนคุณสมบัติของผู้ให้บริการ การดำเนินการช่วงต่อ และความรับผิดต่อความเสียหาย)

กระทรวงดิจิทัลเพื่อเศรษฐกิจและสังคม Ministry of Digital Economy and Society

คู่มือการเลือกใช้ Cloud Computing

หลักเกณฑ์การให้บริการ Cloud Computing

เหตุผลความจำเป็น

- การใช้ Cloud Computing เป็นเทคโนโลยีพื้นฐานในการให้บริการธุรกรรมทางอิเล็กทรอนิกส์
- มีการใช้งานอย่างแพร่หลาย และข้อมูลของหน่วยงานบน Cloud ที่ต้องคำนึงเรื่อง Security + Privacy
- ยังไม่มีหน่วยงานภาครัฐกำหนดนโยบายที่เกี่ยวกับเกณฑ์การให้บริการ Cloud Computing ที่ชัดเจน
- เพื่อส่งเสริมและพัฒนาการให้บริการ Cloud Computing ที่เกี่ยวข้องกับธุรกรรมทางอิเล็กทรอนิกส์ให้มีความมั่นคง ปลอดภัย ความน่าเชื่อถือ สร้างความเชื่อมั่น ลดความเสี่ยงภัยคุกคาม ตลอดจนมีมาตรฐานเป็นที่ยอมรับในระดับสากล
- คณะกรรมการธุรกรรมทางอิเล็กทรอนิกส์ เห็นควรให้กำหนดหลักเกณฑ์การให้บริการ Cloud Computing

หลักการสำคัญในประกาศ

- ส่งเสริมให้เกิดการให้บริการที่มีประสิทธิภาพ
- มีความมั่นคงปลอดภัย เป็นไปตามมาตรฐานสากล
- คำนึงถึงการกำหนดหลักเกณฑ์ที่ชัดเจน การใช้เทคโนโลยีที่เหมาะสม (เป็นกลาง) เพื่อก่อให้เกิดความเชื่อมั่นในการทำธุรกรรมทางอิเล็กทรอนิกส์บน Cloud Computing

หลักเกณฑ์การให้บริการ Cloud Computing

สาระสำคัญ

ขอบเขตประเภทบริการ

	IaaS	Saas	Paas		
1 ฮาร์ดแวร์/อุปกรณ์บันทึก/เครือข่าย	2 ซอฟต์แวร์	3 สภาพแวดล้อมสำหรับการพัฒนาซอฟต์แวร์	4 รวมสองบริการขึ้นไป (1 ถึง 3)	5 บริการอื่นที่ประกาศกำหนด

หลักเกณฑ์

1 การจัดทำนโยบายและแนวทางปฏิบัติขององค์กร (Policy)

- ❑ มาตรการป้องกันกระบวนการทำงาน (Administrative Protection Measures)
- ❑ มาตรการป้องกันทางกายภาพ (Physical Protection)
- ❑ มาตรการป้องกันทางเทคนิค (Technical Protection)

2 ประสิทธิภาพการให้บริการ (Performance)

- ❑ ความพร้อมใช้งาน (Availability)
- ❑ ระยะเวลาการตอบสนอง (Response Time)
- ❑ ความสามารถรองรับปริมาณงาน(Capability)
- ❑ การบริการสนับสนุน (support)
- ❑ กระบวนการยุติสัญญา (Termination Process)

3 การรักษาความมั่นคงปลอดภัย (Security)

- ❑ ความน่าเชื่อถือของบริการ (Reliability)
- ❑ การพิสูจน์ตัวตนและการอนุญาต (Authentication and Authorization)
- ❑ การเข้ารหัส (Encryption)
- ❑ การรายงานเหตุการณ์และการจัดการรักษาความมั่นคงปลอดภัย (Security Incident Management and Reporting)
- ❑ การบันทึกและการตรวจสอบข้อมูลการใช้งานระบบ (Logging and Monitoring)
- ❑ การตรวจสอบขั้นตอนกระบวนการทำงานและความปลอดภัย (Audit and verification)
- ❑ การจัดการช่องโหว่ (Vulnerability Management)
- ❑ ธรรมาภิบาล (Governance)

4 การจัดการข้อมูล (Data Management)

- ❑ การจัดประเภทข้อมูล (Data Classification)
- ❑ การจัดเก็บ สำรองและการเรียกคืนข้อมูล (Storage, Backup and Recovery)
- ❑ วงจรชีวิตของข้อมูล (Lifecycle of Data)
- ❑ การโอนย้ายข้อมูล (Data Export)

5 การคุ้มครองข้อมูลส่วนบุคคล (Data Protection)

- ❑ ปฏิบัติตามมาตรฐานสากล(code of conduct)
- ❑ การระบุวัตถุประสงค์ (Purpose specification)
- ❑ การเก็บรักษาข้อมูลเท่าที่จำเป็น(Data minimization)
- ❑ การใช้ เก็บรักษา และการเปิดเผย (Use, retention and disclosure limitation)
- ❑ ความโปร่งใสและการแจ้งเตือน (Transparency and Notification)
- ❑ ความรับผิดชอบต่อข้อมูล (Accountability)
- ❑ สถานที่จัดเก็บข้อมูล (Data Location)
- ❑ อำนวยความสะดวกการเข้าถึงข้อมูล (Intervenability)

Electronic Transactions Commission

หลักเกณฑ์การให้บริการ Cloud Computing

มาตรฐาน	ความมั่นคงปลอดภัย	ข้อตกลงการให้บริการ (SLA)	ความรับผิดชอบของผู้ให้บริการ
ความน่าเชื่อถือ	การจัดการข้อมูล	ค่าใช้จ่าย	การเลือกใช้งาน
สถานที่เก็บข้อมูล	การคุ้มครองข้อมูล	ประสิทธิภาพการให้บริการ	สำรองข้อมูล

หลักเกณฑ์การให้บริการ Cloud Computing

Electronic Transactions Commission

ขอรับฟังความเห็นในฐานะผู้ใช้บริการ

ขอบเขตประเภทบริการ

	Iaas	Saas	Paas		
1 ฮาร์ดแวร์/อุปกรณ์บันทึก/เครือข่าย	2 ซอฟต์แวร์	3 สภาพแวดล้อมสำหรับการพัฒนาซอฟต์แวร์	4 รวมสองบริการขึ้นไป (1 ถึง 3)	5 บริการอื่นที่ประกาศกำหนด

หลักเกณฑ์

1 การจัดทำนโยบายและแนวทางปฏิบัติขององค์กร (Policy)

- ❑ มาตรการป้องกันกระบวนการทำงาน (Administrative Protection Measures)
- ❑ มาตรการป้องกันทางกายภาพ (Physical Protection)
- ❑ มาตรการป้องกันทางเทคนิค (Technical Protection)

2 ประสิทธิภาพการให้บริการ (Performance)

- ❑ ความพร้อมใช้งาน (Availability)
- ❑ ระยะเวลาการตอบสนอง (Response Time)
- ❑ ความสามารถรองรับปริมาณงาน(Capability)
- ❑ การบริการสนับสนุน (support)
- ❑ กระบวนการยุติสัญญา (Termination Process)

3 การรักษาความมั่นคงปลอดภัย (Security)

- ❑ ความน่าเชื่อถือของบริการ (Reliability)
- ❑ การพิสูจน์ตัวตนและการอนุญาต (Authentication and Authorization)
- ❑ การเข้ารหัส (Encryption)
- ❑ การรายงานเหตุการณ์และการจัดการรักษาความมั่นคงปลอดภัย (Security Incident Management and Reporting)
- ❑ การบันทึกและการตรวจสอบข้อมูลการใช้งานระบบ (Logging and Monitoring)
- ❑ การตรวจสอบขั้นตอนกระบวนการทำงานและความปลอดภัย (Audit and verification)
- ❑ การจัดการช่องโหว่ (Vulnerability Management)
- ❑ ธรรมาภิบาล (Governance)

4 การจัดการข้อมูล (Data Management)

- ❑ การจัดประเภทข้อมูล (Data Classification)
- ❑ การจัดเก็บ สำรองและการเรียกคืนข้อมูล (Storage, Backup and Recovery)
- ❑ วงจรชีวิตของข้อมูล (Lifecycle of Data)
- ❑ การโอนย้ายข้อมูล (Data Export)

5 การคุ้มครองข้อมูลส่วนบุคคล (Data Protection)

- ❑ ปฏิบัติตามมาตรฐานสากล(code of conduct)
- ❑ การระบุวัตถุประสงค์ (Purpose specification)
- ❑ การเก็บรักษาข้อมูลเท่าที่จำเป็น(Data minimization)
- ❑ การใช้ เก็บรักษา และการเปิดเผย (Use, retention and disclosure limitation)
- ❑ ความโปร่งใสและการแจ้งเตือน (Transparency and Notification)
- ❑ ความรับผิดชอบต่อข้อมูล (Accountability)
- ❑ สถานที่จัดเก็บข้อมูล (Data Location)
- ❑ อำนวยความสะดวกการเข้าถึงข้อมูล (Intervenability)

Electronic Transactions Commission

ข้อมูลประกอบ

Electronic Transactions Commission

หลักเกณฑ์การให้บริการ Cloud Computing

1. การจัดทำนโยบายและแนวทางปฏิบัติขององค์กร (Policy)

- **มาตรการป้องกันกระบวนการทำงาน (Administrative Protection Measures)**
  - นโยบายและแนวปฏิบัติว่าด้วยความมั่นคงปลอดภัยสารสนเทศ
  - การพัฒนาทรัพยากรบุคลากรให้มีความรู้ความเข้าใจในเรื่องความมั่นคงปลอดภัยของข้อมูล
  - การประเมินสินทรัพย์ การจัดการเปลี่ยนแปลง การบริหารความเสี่ยง
  - กระบวนการตอบสนองต่อเหตุการณ์ฉุกเฉิน การจัดทำแผนเตรียมความพร้อมกรณีฉุกเฉิน
  - การติดตามดูแลการให้บริการ กระบวนการจ้างช่วงต่อ (สัญญา)
  - และการปฏิบัติอื่นใดตามที่กฎหมายกำหนด
- **มาตรการป้องกันทางกายภาพ (Physical Protection Measures)**
  - การกำหนดควบคุมพื้นที่ ความปลอดภัยในพื้นที่หวงห้าม การควบคุมการเข้าออกพื้นที่
- **มาตรการป้องกันทางเทคนิค (Technical Protection Measures)**
  - ผู้ให้บริการจะต้องจัดให้มีมาตรการในป้องกันสำหรับความมั่นคงปลอดภัยและความน่าเชื่อถือทางเทคนิค
  - โครงสร้างระบบเสมือน (Virtual infrastructure) และสภาพแวดล้อมของระบบ
  - การควบคุมการเข้าถึง การยืนยันตัวตน การตรวจสอบสิทธิของผู้ใช้งานระบบ
  - ความมั่นคงปลอดภัยเครือข่าย
  - การคุ้มครองข้อมูลและการเข้ารหัส
  - การวิเคราะห์ ออกแบบจัดทำระบบตามวัฏจักรการพัฒนาระบบงาน (System development Life Cycle : SDLC)
  - แนวทางในการรักษาความปลอดภัยการจ้างบุคคลภายนอก (Outsourcing)

Electronic Transactions Commission

หลักเกณฑ์การให้บริการ Cloud Computing

2. ประสิทธิภาพการให้บริการ (Performance)

- **ความพร้อมใช้งาน (Availability)**
  ผู้ให้บริการจะต้องแสดงให้ผู้ใช้บริการมั่นใจถึงบริการที่ได้รับ เช่น ร้อยละของเวลาที่พร้อมให้บริการ (Uptime)
- **ระยะเวลาการตอบสนอง (Response Time)**
  ผู้ให้บริการจะต้องระบุระยะเวลาการตอบสนองต่อเหตุการณ์ ซึ่งเป็นระยะเวลานับแต่ผู้ใช้บริการแจ้งความประสงค์และผู้ให้บริการได้ดำเนินการต่อความประสงค์นั้น โดยระยะเวลาการตอบสนองเป็นหลักการพิจารณาที่สำคัญของผู้ใช้บริการ บางกรณีการตอบสนองล่าช้ากว่ากำหนดส่งผลให้เกิดความเสียหาย
- **ความสามารถรองรับปริมาณงาน (Capability)**
  ผู้ให้บริการจะต้องระบุ จำนวนปริมาณการเชื่อมต่อสูงสุดพร้อมกัน จำนวนปริมาณการใช้งานของผู้ใช้บริการพร้อมกัน จำนวนปริมาณทรัพยากรของระบบที่รองรับการใช้งาน และจำนวนปริมาณงาน (Throughput) เพื่อเป็นข้อมูลสำคัญแก่ผู้ใช้บริการ
- **การบริการสนับสนุน (Support)**
  ผู้ให้บริการจะต้องจัดให้มีช่องทางและกำหนดช่วงเวลาที่ผู้ใช้บริการสามารถแจ้งปัญหา หรือติดต่อสอบถามจากผู้ให้บริการได้ เช่น การกำหนดให้ผู้ใช้บริการสามารถติดต่อผู้ให้บริการได้ตลอด 24 ชั่วโมง และระยะเวลาในการแก้ไขปัญหาการใช้งานตั้งแต่เริ่มต้นจนปัญหานั้นสิ้นสุด
- **กระบวนการยุติสัญญา (Termination Process)**
  กรณีผู้ใช้บริการ หรือผู้ให้บริการต้องการยุติข้อตกลงการให้บริการ ผู้ให้บริการจะต้องดำเนินการตามขั้นตอนที่ได้แจ้งให้ผู้ใช้บริการทราบไว้ก่อนล่วงหน้า เช่น ระยะเวลาสำหรับการเข้าถึงข้อมูลของผู้ใช้บริการ และระยะเวลาการเก็บรักษาข้อมูลของผู้ให้บริการ

หลักเกณฑ์การให้บริการ Cloud Computing

3. การรักษาความมั่นคงปลอดภัย (Security)

- **ความน่าเชื่อถือของบริการ (Service Reliability)**
  การควบคุมความมั่นคงปลอดภัย การบริหารจัดการเพื่อความต่อเนื่องทางธุรกิจ และการจัดให้มีระบบฉุกเฉินสำรอง อ้างอิงตามมาตรฐานสากล
- **การพิสูจน์ตัวตนและการอนุญาต (Authentication and Authorization)**
  ตรวจสอบความเป็นตัวตนของผู้มีสิทธิในการเข้าใช้งาน ระยะเวลาเพิ่มหรือถอนสิทธิ์ผู้ใช้งานที่เหมาะสม การป้องกันการเข้าใช้งานจากผู้ที่ไม่มีสิทธิ์ และการควบคุมการเข้าถึงการใช้งานจากบุคคลภายนอกที่สนับสนุนการให้บริการ (Outsourcing)
- **การเข้ารหัส (Encryption)**
  การเข้ารหัสในการแปลงข้อมูลที่มีประสิทธิภาพ เพื่อปกปิดข้อมูล ป้องการเข้าถึง การแก้ไข และการใช้งานโดยไม่ได้รับอนุญาต และจัดให้มีนโยบายการควบคุมกุญแจสำหรับการเข้ารหัส (Key Access Control Policy) ตามความเหมาะสม
- **การรายงานเหตุการณ์และการจัดการรักษาความมั่นคงปลอดภัย (Security Incident Management and Reporting)**
  เนื่องจากการเกิดเหตุการณ์เกี่ยวกับความมั่นคงปลอดภัยของข้อมูลอาจจะส่งผลต่อความมั่นคงทางธุรกิจ โดยการจัดการเหตุการณ์และการรักษาความมั่นคงปลอดภัยของข้อมูล เริ่มตั้งแต่กระบวนการตรวจพบเหตุการณ์ การรายงานเหตุการณ์ การประเมิน การตอบสนอง การแก้ปัญหา และการเรียนรู้จากเหตุการณ์ความปลอดภัยที่เกิดขึ้น
- **การบันทึกและการตรวจสอบข้อมูลการใช้งานระบบ (Logging and Monitoring)**
  การบันทึกข้อมูลที่เกี่ยวข้องกับการดำเนินการและการใช้งานบริการ เพื่อให้สามารถตรวจสอบข้อมูลย้อนหลังได้
- **การตรวจสอบขั้นตอนกระบวนการทำงานและความปลอดภัย** (Audit and verification)
  การตรวจสอบกระบวนการทำงานและความปลอดภัยอย่างเป็นระบบ มีความเป็นอิสระ มีขั้นตอนการทำงานที่มีเอกสารหลักฐาน และกำหนดสิทธิของผู้ตรวจสอบภายใน ผู้ตรวจสอบภายนอก เป็นประจำอย่างสม่ำเสมอ โดยหลักฐานการตรวจสอบที่ใช้และหลักเกณฑ์ถูกกำหนดตามข้อกำหนด หรือตามการรับรองในแต่ละประเภทการให้บริการ
- **การจัดการช่องโหว่ (Vulnerability Management)**
  การตรวจสอบ ประเมิน และบริหารจัดการช่องโหว่ หรือจุดเสี่ยงในระบบ กระบวนการรักษาความปลอดภัยของระบบ การควบคุมภายใน หรือการใช้งานที่อาจถูกนำไปใช้หรือถูกเรียกใช้โดยภัยคุกคาม รวมถึง การทดสอบระบบความปลอดภัย Vulnerability Assessments และ Penetration Testing โดยจะต้องดำเนินการตามมาตรการ และวิธีการที่เหมาะสม เพื่อลดความเสี่ยงในการเกิดความเสียหาย
- **ธรรมาภิบาล (Governance)** กรณีการเปลี่ยนการให้บริการอันเนื่องมากจากการปรับปรุง อัพเดตซอฟต์แวร์ที่อาจส่งผลกระทบกระบวนการทำงาน ช่องทางการให้บริการหรือรายละเอียดในข้อตกลงการให้บริการ ผู้ให้บริการจะต้องมีจัดให้มีการแจ้งให้ผู้ใช้บริการทราบล่วงหน้าในระยะเวลาที่เหมาะสมเพื่อให้ผู้ใช้บริการเตรียมพร้อมในการเปลี่ยนแปลงดังกล่าว

หลักเกณฑ์การให้บริการ Cloud Computing

4. การจัดการข้อมูล (Data Management)

- **การจัดประเภทข้อมูล (Data Classification)**
  - ข้อมูลของผู้ใช้บริการ
  - ข้อมูลของผู้ให้บริการ
  - ข้อมูลที่เกิดจากการประมวลผลข้อมูลของผู้ใช้บริการโดยผู้ให้บริการ (Derived Data)

  ผู้ให้บริการจะต้องจัดให้มีนโยบายที่เกี่ยวข้องกับการใช้ข้อมูลของผู้ใช้บริการ และการกำหนดขอบเขตและแนวปฏิบัติต่อข้อมูลที่ถูกสร้างขึ้นจากข้อมูลของผู้ใช้บริการโดยผู้ให้บริการ โดยกำหนดสิทธิในการตรวจสอบข้อมูลที่เกิดขึ้นของผู้ใช้บริการ
- **การจัดเก็บ สำรองข้อมูล และการเรียกคืนข้อมูล (Storage, Backup and Recovery)**

  ผู้ให้บริการจะต้องจัดให้มีการจัดเก็บสำรองข้อมูลให้อยู่ในสภาพพร้อมใช้งาน โดยกำหนดระยะเวลา ความถี่การดำเนินการ วิธีการ และการเก็บรักษาที่เหมาะสม ในกรณีที่ข้อมูลปัจจุบันถูกทำลายหรือได้รับความเสียหายส่งผลทำให้ไม่สามารถใช้งานได้ผู้ให้บริการจะต้องดำเนินการเรียกคืนข้อมูลเพื่อให้เกิดความพร้อมในการใช้งานตามที่ระบุไว้ในข้อตกลงการให้บริการ
- **วงจรชีวิตของข้อมูล (Lifecycle of Data)**

  ผู้ให้บริการจะต้องจัดให้มีนโยบายและแนวปฏิบัติที่เหมาะสมในการบริหารจัดการข้อมูลอย่างมีประสิทธิภาพและการทำลายข้อมูล
- **การโอนย้ายข้อมูล (Data Export)**

  กรณียุติข้อตกลงการให้บริการ ผู้ให้บริการจะต้องมีนโยบายและแนวปฏิบัติในการส่งออกข้อมูล โดยกำหนดรูปแบบ กระบวนการส่งออกในการโอนย้ายข้อมูลตามความเหมาะสม

Electronic Transactions Commission

หลักเกณฑ์การให้บริการ Cloud Computing

5. การคุ้มครองข้อมูลส่วนบุคคล (Data Protection)

- **แนวปฏิบัติตามมาตรฐานสากล (code of conduct)**
  ผู้ให้บริการจะต้องมีการจัดให้มีนโยบาย แนวทางปฏิบัติ มาตรการ หรือมาตรฐานที่สอดคล้องกับกฎหมายคุ้มครองข้อมูลส่วนบุคคล
- **การระบุวัตถุประสงค์ (Purpose specification)**
  ผู้ให้บริการไม่สามารถดำเนินการกับข้อมูลส่วนบุคคลที่ปราศจากความยินยอมของเจ้าของข้อมูลได้ ทั้งนี้ผู้ให้บริการต้องระบุวัตถุประสงค์และความยินยอมในการรวบรวม เก็บรักษา การใช้ และการเปิดเผยข้อมูล ให้ชัดเจน
- **การเก็บรักษาข้อมูลเท่าที่จำเป็น (Data minimization)**
  ผู้ให้บริการจะต้องมีการกำหนดระยะเวลาในการเก็บรักษาข้อมูลชั่วคราวที่เหมาะสม และการกำหนดระยะเวลาในการเก็บรักษาข้อมูลหลังจากมีการแจ้งให้ทำลายข้อมูล โดยผู้ให้บริการจะต้องระบุให้ชัดเจนในข้อตกลงการให้บริการ ทั้งนี้ ผู้ใช้บริการมีหน้าที่รับผิดชอบต้องตรวจสอบว่าข้อมูลส่วนบุคคลที่ถูกทำลายแล้ว (ทั้งผู้ให้บริการ และผู้รับจ้างต่อ) กรณีข้อมูลชั่วคราวจะถูกสร้างระหว่างการให้บริการ และอาจจะไม่ถูกทำลายในทันที เนื่องจากเหตุผลทางเทคนิค อาจจะต้องตรวจสอบระยะเวลาในการทำลายข้อมูลชั่วคราวด้วย
- **การใช้ เก็บรักษา และการเปิดเผย (Use, retention and disclosure limitation)**
  ผู้ให้บริการจะต้องแจ้งให้ผู้ใช้บริการทราบ ว่าผู้ให้บริการจะไม่เปิดเผยข้อมูลส่วนบุคคลที่มีการจัดเก็บ รวบรวมไว้ เว้นแต่ได้รับความยินยอมจากผู้ใช้บริการ หรือเป็นกรณีที่กฎหมายกำหนดหรือเป็นการเปิดเผยแก่หน่วยงานที่มีอำนาจตามกฎหมาย หรือตามคำสั่งศาล
- **ความโปร่งใส และการแจ้งเตือน (Transparency and Notification)**
  ผู้ให้บริการจะต้องแจ้งให้ผู้ใช้บริการทราบและให้ข้อมูลที่เพียงพอเกี่ยวกับความโปรงใส่ในการดำเนินการกับข้อมูลส่วนบุคคลตามที่กฎหมายกำหนด
- **ความรับผิดชอบต่อข้อมูล (Accountability)**
  เนื่องจากความรับผิดชอบด้านสารสนเทศจะเป็นส่วนสำคัญในการตรวจสอบการละเมิดข้อมูลส่วนบุคคล ผู้ให้บริการจะต้องมีนโยบายและแนวปฏิบัติในกรณีการละเมิดข้อมูล และจะต้องมีกระบวนการ เอกสารหลักฐานที่ได้ดำเนินการที่สอดคล้องกับแนวทางการคุ้มครองข้อมูลส่วนบุคคล
- **สถานที่จัดเก็บข้อมูล (Data Location)**
  การประมวลผลข้อมูลส่วนบุคคลอาจจะถูกโอนย้ายข้อมูลไปยังต่างประเทศซึ่งอาจจะมีกฎหมาย กฎระเบียบหรือระดับความการคุ้มครองข้อมูลส่วนบุคคลที่แตกต่างกัน เพื่อเป็นการลดความเสี่ยงในการถูกละเมิด ผู้ให้บริการจะต้องแสดงให้ผู้ใช้บริการทราบสถานที่ในการจัดเก็บข้อมูล หรือกำหนดให้ผู้ใช้บริการสามารถเลือกสถานที่จัดเก็บข้อมูลได้
- **อำนวยความสะดวกการเข้าถึงข้อมูล** (Intervenability) ผู้ให้บริการจะต้องมีหน้าที่ในการอำนวยความสะดวกแก่ผู้ใช้บริการในระยะเวลาเหมาะสมและมีประสิทธิภาพ ทั้งนี้ ห้ามมิให้ผู้ให้บริการใช้ข้อกำหนดทางเทคนิคหรือข้อกำหนดขององค์กรเป็นอุปสรรคในการปฏิเสธสิทธิของเจ้าของข้อมูล

Electronic Transactions Commission

มาตรฐานที่เกี่ยวกับ Cloud Computing